McAfee®

Internet Security Suite 2008

Brukerhåndbok

Innhold

McAfee Internet Security 3

McAfee SecurityCenter ... 5
SecurityCenter-funksjoner ... 6
Bruke SecurityCenter ... 7
Oppdatere SecurityCenter ... 13
Reparere eller ignorere beskyttelsesproblemer ... 17
Arbeide med varsler ... 23
Vise hendelser ... 29
McAfee VirusScan ... 31
VirusScan-funksjoner ... 32
Starte sanntids virusbeskyttelse ... 33
Starte tilleggsbeskyttelse ... 35
Konfigurere virusbeskyttelse ... 39
Gjennomsøke datamaskinen ... 57
Arbeide med søkeresultater ... 61
McAfee Personal Firewall ... 65
Personal Firewall-funksjoner ... 66
Starte Firewall ... 69
Arbeide med varsler ... 71
Håndtere informasjonsvarsler ... 75
Konfigurere Firewall-beskyttelse ... 77
Administrere programmer og tillatelser ... 89
Behandle systemtjenester ... 97
Administrere datamaskintilkoblinger ... 103
Logge, overvåke og analysere ... 111
Lære om Internett-sikkerhet ... 121
McAfee Anti-Spam ... 123
Anti-Spam-funksjoner ... 125
Konfigurere webpostkontoer ... 127
Konfigurere venner ... 131
Konfigurere spamoppdagelse ... 137
E-postfiltrering ... 145
Arbeide med filtrert e-post ... 149
Konfigurere beskyttelse mot phishing ... 151
McAfee Privacy Service ... 153
Privacy Service-funksjoner ... 154
Sette opp foreldrestyring ... 155
Beskytte opplysninger på Internett ... 171
Beskytte passord ... 173
McAfee Data Backup ... 177
Funksjoner ... 178
Arkivere filer ... 179
Arbeide med arkiverte filer ... 187
McAfee QuickClean ... 193
QuickClean-funksjoner ... 194
Rens av datamaskinen ... 195
Defragmentering av datamaskinen ... 198

Planlegging av oppgave 199
McAfee Shredder 205
Shredder-funksjoner 206
Makulering av filer, mapper og disker 207
McAfee Network Manager 209
Network Manager funksjoner 210
Forstå Network Manager-ikoner 211
Sette opp et administrert nettverk 213
Administrere nettverket eksternt 221
McAfee EasyNetwork 227
EasyNetwork funksjoner 228
Konfigurere EasyNetwork 229
Dele og sende filer 235
Dele skrivere 241
Referanse 243

Liste 244

Om McAfee 259

Copyright 259
Lisens 260
Kundestøtte og teknisk støtte 261
Bruke McAfee Virtuell tekniker 262
Støtte og nedlastninger 263

Indeks 272

KAPITTEL 1

McAfee Internet Security

McAfee® Internet Security Suite med SiteAdvisor er en proaktiv pakke av 10-i-1-sikkerhetssystemer som alltid er oppdatert og som beskytter det du setter pris på, identiteten og datamaskinen din, mot virus, spionprogrammer, svindel via e-post og direktemeldinger, hackere og overgripere, og som samtidig tilbyr automatisk sikkerhetskopiering av viktige filer. Du kan føle deg trygg når du surfer på nettet, handler, bruker nettbank, e-post og direktemeldinger og laster ned filer. McAfee SiteAdvisor og foreldresstyring hjelper deg og familien med å unngå usikre nettsteder. McAfees sikkerhetssystem leverer oppdaterte funksjoner, forbedringer og trusselinformasjon kontinuerlig og automatisk. PC-en blir også automatisk trimmet, slik at unødvendige filer blir fjernet og PC-en alltid har topp ytelse.

I dette kapitlet

McAfee SecurityCenter 5
McAfee VirusScan 31
McAfee Personal Firewall 65
McAfee Anti-Spam 123
McAfee Privacy Service 153
McAfee Data Backup 177
McAfee QuickClean 193
McAfee Shredder 205
McAfee Network Manager 209
McAfee EasyNetwork 227
Referanse 243
Om McAfee 259
Kundestøtte og teknisk støtte 261

KAPITTEL 2

McAfee SecurityCenter

McAfee SecurityCenter lar deg overvåke sikkerhetsstatusen til datamaskinen din, øyeblikkelig finne ut om din datamaskins tjenester for virus-, spionprogram-, e-post- og brannmurbeskyttelse er oppdatert, og reparere potensielle sikkerhetshull. Det gir deg navigeringsverktøyene og kontrollene du trenger for å koordinere og administrere alle områder av din datamaskins beskyttelse.

Før du starter konfigurering og administrering av din datamaskins beskyttelse, gå gjennom SecurityCenter-grensesnittet og forsikre deg om at du forstår forskjellen mellom beskyttelsesstatus, beskyttelseskategorier og beskyttelsestjenester. Oppdater deretter SecurityCenter for å forsikre deg om at du har den siste tilgjengelige beskyttelsen fra McAfee.

Etter at de første konfigurasjonsoppgavene er fullført, bruker du SecurityCenter til å overvåke beskyttelsesstatusen til din datamaskin. Hvis SecurityCenter oppdager et beskyttelsesproblem varsler det deg slik at du enten kan fikse eller ignorere problemet (avhengig av hvor alvorlig det er). Du kan også gå gjennom hendelser i SecurityCenter, som konfigurasjonsendringer i virusskanning, i en hendelseslogg.

Merknad: SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer så snart det oppdager dem. Hvis du trenger hjelp til å diagnostisere beskyttelsesproblemene, kan du kjøre McAfee Virtual Technician.

I dette kapitlet

SecurityCenter-funksjoner 6
Bruke SecurityCenter 7
Oppdatere SecurityCenter 13
Reparere eller ignorere beskyttelsesproblemer 17
Arbeide med varsler 23
Vise hendelser 29

SecurityCenter-funksjoner

SecurityCenter har følgende funksjoner:

Forenklet beskyttelsesstatus

Gjør det enkelt å gå gjennom datamaskinens sikkerhetsstatus, se etter oppdateringer og fikse potensielle sikkerhetsproblemer.

Kontinuerlige oppdateringer og oppgraderinger

Automatisk nedlasting og installering av oppdateringer til dine registrerte programmer. Når en ny versjon av et registrert McAfee-program er tilgjengelig, får du den automatisk gratis tilsendt når du abonnerer, slik at du alltid er sikret den mest oppdaterte beskyttelsen.

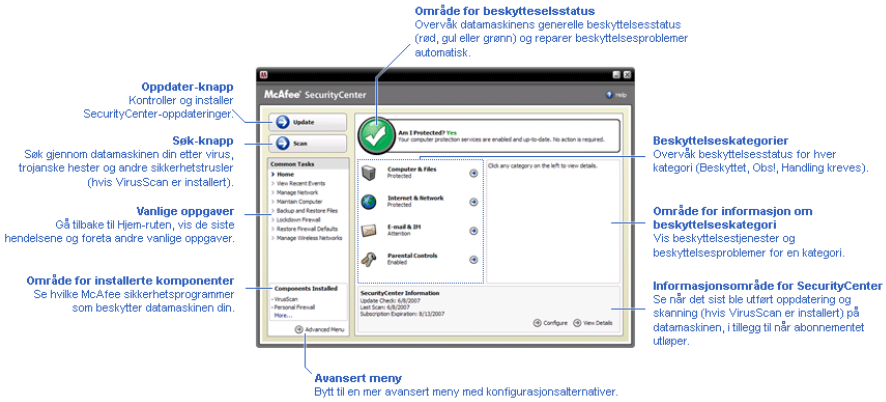
Sanntidsvarsling

Sikkerhetsvarsling varsler deg om kritiske virusutbrudd og sikkerhetstrusler og gir deg mulighet til å fjerne, nøytralisere eller lære mer om trusselen.

KAPITTEL 3

Bruke SecurityCenter

Før du begynner å bruke SecurityCenter, gå gjennom komponentene og konfigurasjonsområdene du skal bruke til å administrere din datamaskins beskyttelsesstatus. For mer informasjon om terminologien som er brukt i dette bildet, se Forstå beskyttelsesstatus (side 8) og Forstå beskyttelseskategorier (side 9). Du kan så gå gjennom kontoinformasjonen din for McAfee og bekreft abonnementet ditt.



I dette kapitlet

Forstå beskyttelsesstatus 8
Forstå beskyttelseskategorier 9
Forstå beskyttelsestjenester 10
Administrere din McAfee-konto 11

Forstå beskyttelsesstatus

Beskyttelsesstatusen til datamaskinen din vises i området for beskyttelsesstatus i Hjem-ruten i SecurityCenter. Den viser om datamaskinen din er fullstendig beskyttet mot de siste sikkerhetstruslene og kan påvirkes av ting som eksterne sikkerhetsangrep, andre sikkerhetsprogrammer og programmer som har tilgang til Internett.

Beskyttelsesstatusen til din datamaskin kan være rød, gul eller grønn.

Beskyttelses-status	Beskrivelse
Rød	Datamaskinen er ikke beskyttet. Området for beskyttelsesstatus i Hjem-ruten i SecurityCenter er rød og viser at du ikke er beskyttet. SecurityCenter rapporterer om minst ett kritisk sikkerhetsproblem. For å oppnå fullstendig beskyttelse må du reparere alle kritiske sikkerhetsproblemer i hver beskyttelseskategori (problemkategoriens status er satt til **Handling kreves**, også i rødt). For informasjon om hvordan du reparerer beskyttelsesproblemer, se Løse beskyttelsesproblemer (side 18).
Gul	Datamaskinen er delvis beskyttet. Området for beskyttelsesstatus i Hjem-ruten i SecurityCenter er gul og viser at du ikke er beskyttet. SecurityCenter rapporterer om minst ett ikke-kritisk sikkerhetsproblem. For å oppnå fullstendig beskyttelse må du reparere eller ignorere de ikke-kritiske sikkerhetsproblemene i hver beskyttelseskategori. For informasjon om hvordan du reparerer eller ignorerer beskyttelsesproblemer, se Løse eller ignorere beskyttelsesproblemer (side 17).
Grønn	Datamaskinen er fullstendig beskyttet. Området for beskyttelsesstatus i Hjem-ruten i SecurityCenter er grønn og viser at du er beskyttet. SecurityCenter rapporterer ikke om noen kritiske eller ikke-kritiske sikkerhetsproblemer. Hver beskyttelseskategori oppgir tjenestene som beskytter datamaskinen din.

Forstå beskyttelseskategorier

SecurityCenters beskyttelsestjenester er delt inn i fire kategorier: Datamaskin & Filer, Internett & Nettverk, E-post & direktemeldinger og foreldrestyring. Disse kategoriene hjelper deg å bla gjennom og konfigurere sikkerhetstjenestene som beskytter datamaskinen din.

Du klikker på et kategorinavn for å konfigurere beskyttelsestjenestene og se sikkerhetsproblemer som er oppdaget for disse tjenestene. Hvis beskyttelsesstatusen til din datamaskin er rød eller gul, vil en eller flere kategorier vise beskjeden *Handling kreves* eller *Obs*, som indikerer at SecurityCenter har oppdaget et problem med kategorien. For mer informasjon om beskyttelsesstatus, se Forstå beskyttelsesstatus (side 8).

Beskyttelses-kategori	Beskrivelse
Datamaskin og filer	Kategorien Datamaskin og filer lar deg konfigurere følgende beskyttelsestjenester: ▪ Virusbeskyttelse ▪ Beskyttelse mot potensielt uønskede program (PUP) ▪ Systemovervåking ▪ Windows-beskyttelse
Internett og nettverk	Kategorien Internett og nettverk lar deg konfigurere følgende beskyttelsestjenester: ▪ Brannmurbeskyttelse ▪ Identitetsbeskyttelse
E-post og direktemeldinger	Kategorien E-post og direktemeldinger lar deg konfigurere følgende beskyttelsestjenester: ▪ E-post-beskyttelse ▪ Spambeskyttelse
Foreldrestyring	Kategorien Foreldrestrying lar deg konfigurere følgende beskyttelsestjenester: ▪ Innholdsblokkering

Forstå beskyttelsestjenester

Beskyttelsestjenester er SecurityCenters kjernekomponenter som du konfigurerer til å beskytte datamaskinen din. Beskyttelsestjenester korresponderer direkte med McAfee-programmer. For eksempel, når du installerer VirusScan, blir følgende beskyttelsestjenester tilgjengelig: Virusbeskyttelse, beskyttelse mot potensielle uønskede programmer (PUP), Systemovervåking og Windows-beskyttelse. For detaljert informasjon om disse bestemte beskyttelsestjenestene, se Hjelp for VirusScan.

Som standardinnstilling er alle beskyttelsestjenester tilknyttet et program aktivert når du installerer programmet; du kan imidlertid deaktivere en beskyttelsestjeneste når som helst. For eksempel, hvis du installerer Privacy Service vil både Innholdsblokkering og Identitetsbeskyttelse være aktivert. Hvis du ikke har tenkt å bruke beskyttelsestjenesten Innholdsblokkering, kan du deaktivere den fullstendig. Du kan også midlertidig deaktivere en beskyttelsestjeneste mens du utfører installasjon eller vedlikeholdsoppgaver.

Administrere din McAfee-konto

Administrer din McAfee-konto fra SecurityCenter ved å enkelt få tilgang til og gå gjennom din kontoinformasjon og bekrefte din nåværende abonnementsstatus.

Merknad: Hvis du installerte McAfee-programmene dine fra en CD, må du registrere dem på McAfees webområde for å konfigurere eller oppdatere din McAfee-konto. Bare da får du tilgang til faste, automatiske programoppdateringer.

Administrere din McAfee-konto

Du kan enkelt få tilgang til informasjonen i din McAfee-konto (Min konto) fra SecurityCenter.

1. Under **Vanlige oppgaver** klikker du **Min konto**.
2. Logg inn på din McAfee-konto.

Bekreft abonnementet

Du bekrefter abonnementet for å kontrollere at det ikke har gått ut.

- Høyreklikk SecurityCenter-ikonet i systemstatusfeltet helt til høyre på oppgavelinjen, og klikk deretter på **Bekreft abonnement**.

KAPITTEL 4

Oppdatere SecurityCenter

SecurityCenter sørger for at dine registrerte McAfee-programmer er oppdaterte ved å se etter og installere oppdateringer på nettet hver fjerde time. Avhengig av programmene du har installert og regisrert, kan oppdateringer fra nettet inkludere de siste virusdefinisjonene og oppgraderinger for hacker-, spam-, spionprogram- og personvernbeskyttelser. Hvis du ønsker å se etter oppdateringer innenfor firetimersperioden som er standard, kan du gjøre dette når som helst. Mens SecurityCenter ser etter oppdateringer, kan du fortsette å utføre andre oppgaver.

Selv om det ikke er anbefalt, kan du endre måten SecurityCenter se etter or installerer oppdateringer. For eksempel kan du konfigurere SecurityCenter til å laste ned, men ikke installere oppdateringer, eller si ifra før det laster ned eller installerer oppdateringer. Du kan også deaktivere automatisk oppdatering.

Merknad: Hvis du installerte McAfee-programmene fra en CD, kan du ikke motta faste, automatiske oppdateringer for disse programmene med mindre du registrerer dem på McAfees webområde.

I dette kapitlet

Se etter oppdateringer 13
Konfigurere automatiske oppdateringer 14
Deaktivere automatiske oppdateringer 14

Se etter oppdateringer

Som standardinnstilling ser SecurityCenter automatisk etter oppdateringer hver fjerde time når datamaskinen din er tilkoblet Internett; hvis du imidlertid ønsker å se etter oppdateringer innenfor firetimersperioden kan du gjøre dette. Hvis du har deaktivert automatiske oppdateringer er det ditt ansvar å se etter oppdateringer med jevne mellomrom.

- Klikk **Oppdater** i Hjem-ruten i SecurityCenter.

Tips: Du kan se etter oppdateringer uten å starte SecurityCenter ved å høyreklikke SecurityCenter-ikonet i systemstatusfeltet helt til høyre på oppgavelinjen, og så klikke på **Oppdateringer**.

Konfigurere automatiske oppdateringer

Som standardinnstilling ser SecurityCenter automatisk etter oppdateringer og installerer dem hver fjerde time når du er tilkoblet Internett. Hvis du ønsker å endre denne standardinnstilingen kan du konfigurere SecurityCenter til å automatisk laste ned oppdateringer og gi beskjed når oppdateringene er klare til å installeres, eller gi beskjed før oppdateringer lastes ned.

Merknad: SecurityCenter gir deg beskjed via varsler når oppdateringer er klare til å lastes ned eller installeres. Fra varslene kan du enten laste ned eller installere oppdateringene, eller utsette oppdateringene. Når du oppdaterer programmene fra et varsel, kan det hende du må bekrefte abonnementet ditt før du kan laste ned og installere. For mer informasjon, se Arbeide med varsler (side 23).

1. Åpne konfigurasjonsruten for SecurityCenter

   Hvordan?

   1. Under **Vanlige oppgaver** klikker du **Hjem**.
   2. Klikk **Konfigurer** i den høyre ruten under **SecurityCenter-informasjon**.

2. I konfigurasjonsruten for SecurityCenter, under **Automatiske oppdateringer er deaktiverte**, klikk på **På**, og klikk deretter på **Avansert**.
3. Klikk én av følgende knapper:
   - **Installer oppdateringene automatisk, og varsle meg når tjenestene er oppdatert (anbefales)**
   - **Last ned oppdateringene automatisk, og varsle meg når de er klare til å installeres**
   - **Varsle meg før oppdateringer lastes ned**
4. Klikk **OK**.

Deaktivere automatiske oppdateringer

Hvis du deaktiverer automatiske oppdateringer er det ditt ansvar å se etter oppdateringer med jevne mellomrom; hvis ikke vil ikke datamaskinen ha den siste sikkerhetsbeskyttelsen. For informasjon om hvordan du ser etter oppdateringer manuelt, se Se etter oppdateringer (side 13).

1. Åpne konfigurasjonsruten for SecurityCenter

   Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. Klikk **Konfigurer** i den høyre ruten under **SecurityCenter-informasjon**.

2 I konfigurasjonsruten for SecurityCenter, under **Automatiske oppdateringer er aktivert**, klikk på **Av**.

Tips: Du aktiverer automatiske oppdateringer ved å klikke på **På**-knappen eller ved å fjerne **Deaktiver automatisk oppdatering og la meg se etter oppdateringer manuelt** i ruten for Oppdateringsalternativer.

KAPITTEL 5

Reparere eller ignorere beskyttelsesproblemer

SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer så snart det oppdager dem. Kritiske beskyttelsesproblemer krever øyeblikkelig handling og kan sette din beskyttelsesstatus på spill (endre fargen til rød). Ikke-kritiske beskyttelsesproblemer krever ikke øyeblikkelig handling og kan kanskje sette din beskyttelsesstatus på spill (avhengig av hva slags type problem det dreier seg om). For å oppnå grønn beskyttelsesstatus må du reparere alle kritiske problemer og enten reparere eller ignorere alle ikke-kritiske problemer. Hvis du trenger hjelp til å diagnostisere beskyttelsesproblemene, kan du kjøre McAfee Virtuell Tekniker. For mer informasjon om McAfee Virtuell tekniker, se Hjelp for McAfee Virtuell tekniker.

I dette kapitlet

Løse beskyttelsesproblemer 18
Ignorere beskyttelsesproblemer 20

Løse beskyttelsesproblemer

De fleste sikkerhetsproblemer kan repareres automatisk; noen problemer kan imidlertid kreve handling. For eksempel, hvis Brannmurbeskyttelse er deaktivert, kan SecurityCenter aktivere den automatisk; men hvis Brannmurbeskyttelse ikke er installert, må du installere den. Følgende tabell beskriver flere handlinger du kan utføre når du skal reparere beskyttelsesproblemer manuelt:

Problem	Handling
Det er ikke fullført et fullstendig søk på datamaskinen de siste 30 dagene.	Gjennomsøk datamaskinen manuelt For mer informasjon, se Hjelp for VirusScan.
Dine signaturfiler for oppdagelse (DAT-filer) er utdaterte.	Oppdater beskyttelsen manuelt. For mer informasjon, se Hjelp for VirusScan.
Et program er ikke installert.	Installer programmet fra McAfees webområde eller CD.
Et program mangler komponenter.	Reinstaller programmet fra McAfees webområde eller CD.
Et program er ikke registrert, og kan ikke oppnå fullstendig beskyttelse.	Registrer programmet på McAfees webområde.
Et program er utløpt.	Kontroller statusen til din konto på McAfees webområde.

Merknad: Ofte påvirker ett enkelt beskyttelsesproblem mer enn én beskyttelseskategori. Hvis dette er tilfelle, fjernes problemet fra alle beskyttelseskategorier når du reparerer det i én kategori.

Løse beskyttelsesproblemer automatisk

SecurityCenter kan løse de fleste beskyttelsesproblemene automatisk. Konfigurasjonsendringene som SecurityCenter gjør når det løser beskyttelsesproblemer automatisk, blir ikke registrert i hendelsesloggen. For mer informasjon om varsler, se Om varsler (side 29).

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. I området for beskyttelsesstatus i Hjem-ruten i SecurityCenter klikker du **Reparer**.

Løse beskyttelsesproblemer manuelt

Hvis ett eller flere beskyttelsesproblemer vedvarer etter at du har forsøkt å løse dem automatisk, kan du løse problemene manuelt.

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. I Hjem-ruten i SecurityCenter klikker du på den beskyttelseskategorien SecurityCenter rapporterer om problemet i.
3. Klikk på koblingen etter beskrivelsen av problemet.

Ignorere beskyttelsesproblemer

Hvis SecurityCenter oppdager et ikke-kritisk problem kan du enten løse eller ignorere det. Andre ikke-kritiske problemer (f.eks. hvis Anti-Spam eller Privacy Service ikke er installert) ignoreres automatisk. Ignorerte problemer vises ikke i informasjonsområdet for beskyttelseskategorier i Hjem-ruten i SecurityCenter med mindre beskyttelsesstatusen til datamaskinen er grønn. Hvis du ignorerer et problem, men senere vil at det skal vises i informasjonsområdet for beskyttelseskategorier selv når beskyttelsesstatusen til datamaskinen ikke er grønn, kan du vise det ignorerte problemet.

Ignorere et beskyttelsesproblem

Hvis SecurityCenter oppdager et ikke-kritisk problem du ikke har planer om å løse, kan du ignorere det. Når du ignorerer problemet fjernes det fra informasjonsområdet for beskyttelseskategorier i SecurityCenter.

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. I Hjem-ruten i SecurityCenter klikker du på den beskyttelseskategorien SecurityCenter rapporterer om problemet i.
3. Klikk på **Ignorer** -koblingen ved siden av beskyttelsesproblemet.

Vis eller skjul ignorerte problemer

Du kan vise eller skjule et ignorert beskyttelsesproblem, avhengig av hvor alvorlig det er.

1. Åpne ruten Varslingsalternativer.

   Hvordan?

   1. Under **Vanlige oppgaver** klikker du **Hjem**.
   2. Klikk **Konfigurer** i den høyre ruten under **SecurityCenter-informasjon**.
   3. Under **Varsler** klikker du **Avansert**.
2. I ruten SecurityCenter-konfigurasjon klikker du på **Ignorerte problemer**.
3. I ruten Ignorerte problemer gjør du følgende:
   - Hvis du vil ignorere et problem merker du av i avmerkingsboksen.
   - Hvis du vil rapportere et problem i informasjonsområdet for beskyttelseskategorier, fjerner du merket i avmerkingsboksen.

4 Klikk **OK**.

Tips: Du kan også ignorere et problem ved å klikke på **Ignorer**-koblingen ved siden av det rapporterte problemet i informasjonsområdet for beskyttelseskategorier.

KAPITTEL 6

Arbeide med varsler

Varsler er små popup-dialogbokser som vises i nederste høyre hjørne av skjermen når SecurityCenter-hendelser oppstår. Et varsel viser detaljert informasjon om en hendelse, samt anbefalinger og valg for å løse problemer som kan være tilkyttet hendelsen. Noen varsler inneholder også koblinger til ytterligere informasjon om hendelsen. Disse koblingene lar deg starte McAfees globale webområde eller sende informasjon til McAfee for feilsøking.

Det finnes tre typer varsler: rød, gul og grønn.

Varseltype	Beskrivelse
Rød	Et rødt varsel er en kritisk melding som krever en handling fra deg. Røde varsler oppstår når SecurityCenter ikke kan fastslå hvordan det kan løse et problem automatisk.
Gul	Et gult varsel er en ikke-kritisk melding som vanligvis krever en handling fra deg.
Grønn	Et grønt varsel er en ikke-kritisk melding som ikke krever en handling fra deg. Grønne varsler gir deg grunnleggende informasjon om en hendelse.

Siden varsler er svært viktige når du overvåker og administrerer beskyttelsesstatusen, kan du ikke deaktivere dem. Du kan imidlertid bestemme om visse typer informasjonsvarsler skal vises og konfigurere noen andre varslingsvalg (f.eks. om SecurityCenter skal spille av en lyd med et varsel eller vise McAfees velkomstskjerm ved oppstart).

I dette kapitlet

Vise og skjule informasjonsvarsler.....24
Konfigurere varslingsalternativer 26

Vise og skjule informasjonsvarsler

Informasjonsvarsler gir deg beskjed når det oppstår hendelser som ikke utgjør en trussel mot datamaskinens sikkerhet. Hvis du f.eks. har installert Brannmurbeskyttelse vises som standard et informasjonsvarsel hver gang et program på datamaskinen blir gitt tilgang til Internett. Hvis du ikke vil at en bestemt type informasjonsvarsler skal vises, kan du skjule dem. Hvis du ikke vil at noen informasjonsvarsler skal vises, kan du skjule alle. Du kan også skjule alle informasjonsvarsler når du spiller spill i fullskjermmodus på datamaskinen. Når du er ferdig med spillet og går ut av fullskjermmodus fortsetter SecurityCenter å vise informasjonsvarsler.

Hvis du skjuler et informasjonsvarsel ved et uhell, kan du vise det igjen når som helst. Som standardinnstilling viser SecurityCenter alle informasjonsvarsler.

Vise eller skjule informasjonsvarsler

Du kan konfigurere SecurityCenter til å vise noen informasjonsvarsler og skjule andre, eller til å skjule alle informasjonsvarsler.

1. Åpne ruten Varslingsalternativer.

   Hvordan?

   1. Under **Vanlige oppgaver** klikker du **Hjem**.
   2. Klikk **Konfigurer** i den høyre ruten under **SecurityCenter-informasjon**.
   3. Under **Varsler** klikker du **Avansert**.

2. I ruten SecurityCenter-konfigurasjon klikker du på **Informasjonsvarsler**.
3. I ruten Informasjonsvarsler gjør du følgende:
   - Hvis du vil vise et informasjonsvarsel, fjerner du merket i avmerkingsboksen.
   - Hvis du vil skjule et informasjonsvarsel, merker du av i avmerkingsboksen.
   - Hvis du vil skjule alle informasjonsvarsler merker du av i boksen **Ikke vis informasjonsvarsler**.
4. Klikk **OK**.

Tips: Du kan også skjule et informasjonsvarsel ved å merke av i boksen **Ikke vis dette varslet igjen** i selve varslet. Hvis du gjør dette kan du vise informasjonsvarslet igjen ved å fjerne merket i den korresponderende avmerkingsboksen i ruten Informasjonsvarsler.

Vise eller skjule informasjonsvarsler når du spiller

Du kan skjule informasjonsvarsler når du spiller spill i fullskjermmodus på datamaskinen. Når du er ferdig med spillet og går ut av fullskjermmodus fortsetter SecurityCenter å vise informasjonsvarsler igjen.

1 Åpne ruten Varslingsalternativer.

Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. Klikk **Konfigurer** i den høyre ruten under **SecurityCenter-informasjon**.
3. Under **Varsler** klikker du **Avansert**.

2 I ruten Varslingsalternativer merker du av eller fjerner merket i boksen **Show informational alerts when gaming mode is detected**.

3 Klikk **OK**.

Konfigurere varslingsalternativer

Varslenes visning og hyppighet konfigureres av SecurityCenter; du kan imidlertid justere noen grunnleggende varslingsalternativer. Du kan f.eks. spille av en lyd med varsler eller skjule velkomstskjermvarslet når Windows starter. Du kan også skjule varsler som melder fra om virusutbrudd og andre sikkerhetstrusler i Internett-samfunn.

Spille av en lyd med varsler

Hvis du vil ha en hørbar indikasjon på at et varsel har oppstått, kan du konfigurere SecurityCenter til å spille av en lyd med hvert varsel.

1 Åpne ruten Varslingsalternativer.

Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. Klikk **Konfigurer** i den høyre ruten under **SecurityCenter-informasjon**.
3. Under **Varsler** klikker du **Avansert**.

2 Under **Lyd** i ruten Varslingsalternativer merker du av i boksen for **Spill av en lyd når det oppstår varsler**.

Skjule velkomstskjermen ved oppstart

Som standardinnstilling vises McAfees velkomstskjerm kort når Windows starter, for å informere deg om at SecurityCenter beskytter datamaskinen. Du kan imidlertid skjule velkomstskjermen hvis du ikke vil at den skal vises.

1 Åpne ruten Varslingsalternativer.

Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. Klikk **Konfigurer** i den høyre ruten under **SecurityCenter-informasjon**.
3. Under **Varsler** klikker du **Avansert**.

2 Under **Velkomstskjerm** i ruten Varslingsalternativer fjerner du merket i boksen for **Vis McAfees velkomstskjerm når Windows starter**.

Tips: Du kan når som helst vise velkomstskjermen igjen ved å merke av i boksen for **Vis McAfees velkomstskjerm når Windows starter**.

Skjule virusutbrudd-varsler

Du kan skjule varsler som melder fra om virusutbrudd og andre sikkerhetstrusler i Internett-samfunn.

1 Åpne ruten Varslingsalternativer.

Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. Klikk **Konfigurer** i den høyre ruten under **SecurityCenter-informasjon**.
3. Under **Varsler** klikker du **Avansert**.

2 I ruten Varslingsalternativer fjerner du merket i boksen **Varsle meg når det oppstår et virus eller en sikkerhetstrussel**.

Tips: Du kan vise virusutbrudd-varsler når som helst ved å merke av i boksen **Varsle meg når det oppstår et virus eller en sikkerhetstrussel**.

KAPITTEL 7

Vise hendelser

En hendelse er en handling eller konfigurasjonsendring som oppstår i en beskyttelseskategori og dens tilknyttede beskyttelsestjenester. Ulike beskyttelsestjenester registrerer ulike typer hendelser. For eksempel registrerer SecurityCenter en hendelse hvis en beskyttelsestjeneste blir aktivert eller deaktivert; Virusbeskyttelse registrerer en hendelse hver gang et virus blir oppdaget og fjernet, og Brannmurbeskyttelse registrerer en hendelse hver gang et forsøk på å koble til Internett blir blokkert. For mer informasjon om beskyttelseskategorier, se Forstå beskyttelseskategorier (side 9).

Du kan se hendelser når du foretar feilsøking i konfigureringsspørsmål og går gjennom handlinger utført av andre brukere. Mange foreldre bruker hendelsesloggen til å overvåke barnas oppførsel på Internett. Hvis du kun vil undersøke de siste 30 hendelsene som har oppstått, viser du nyeste hendelser. Hvis du vil undersøke en omfattende liste over alle hendelser som har oppstått, viser du alle hendelser. Når du viser alle hendelser, åpner SecurityCenter hendelsesloggen, som sorterer hendelser etter beskyttelseskategoriene de oppsto i.

I dette kapitlet

Vise nylige hendelser 29
Vise alle hendelser.....30

Vise nylige hendelser

Hvis du kun vil undersøke de siste 30 hendelsene som har oppstått, viser du nyeste hendelser.

- Under **Vanlige oppgaver,** klikker du **Vis nyeste hendelser**.

Vise alle hendelser

Hvis du vil undersøke en omfattende liste over alle hendelser som har oppstått, viser du alle hendelser.

1. Under **Vanlige oppgaver,** klikker du **Vis nyeste hendelser**.
2. Klikk **Vis logg** i ruten Nylige hendelser.
3. I hendelsesloggens venstre rute klikker du hvilke typer hendelser du vil vise.

KAPITTEL 8

McAfee VirusScan

VirusScan tilbyr avanserte tjenester for oppdagelse og beskyttelse som forsvarer deg og din datamaskin mot de siste sikkerhetstruslene, inkludert virus, trojanske hester, informasjonskapsler for sporing, spion- og reklameprogrammer og andre potensielt uønskede programmer. Med VirusScan rekker beskyttelsen lenger enn filene og mappene på din stasjonære eller bærbare datamaskin, og programmet går etter trusler fra ulike inngangspunkt, inkludert e-post, direktemeldinger og Internett.

Med VirusScan er beskyttelsen av datamaskinen din øyeblikkelig og konstant (krever ingen langtekkelig administrering). Mens du arbeider, spiller, surfer på Internett eller leser e-post kjører det i bakgrunnen og overvåker, søker etter og oppdager potensielle skader i sanntid. Omfattende søk gjennomføres etter tidsskjema og sjekker datamaskinen din jevnlig ved bruk av et avansert sett alternativer. VirusScan gir deg fleksibilitet til å tilpasse hvordan programmet skal fungere, men selv om du ikke gjør det vil datamaskinen din likevel være beskyttet.

Ved normal bruk av datamaskinen kan virus, ormer og and potensielle trusler infiltrere datamaskinen. Dersom dette skjer varsler VirusScan deg om trusselen, men vil vanligvis ta seg av den for deg ved å fjerne eller isolere infiserte elementer før skade oppstår. Selv om det er sjelden, kan videre handling noen ganger være nødvendig. I slike tilfeller lar VirusScan deg bestemme hva du skal gjøre (søke på nytt neste gang du slår på datamaskinen, beholde det oppdagede elementet eller fjerne det oppdagede elementet).

Merknad: SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer så snart det oppdager dem. Hvis du trenger hjelp til å diagnostisere beskyttelsesproblemene, kan du kjøre McAfee Virtual Technician.

I dette kapitlet

VirusScan-funksjoner 32
Starte sanntids virusbeskyttelse 33
Starte tilleggsbeskyttelse.....35
Konfigurere virusbeskyttelse 39
Gjennomsøke datamaskinen 57
Arbeide med søkeresultater.....61

VirusScan-funksjoner

VirusScan har følgende funksjoner.

Omfattende virusbeskyttelse

VirusScan tilbyr avanserte tjenester for oppdagelse og beskyttelse som forsvarer deg og din datamaskin mot de siste sikkerhetstruslene, inkludert virus, trojanske hester, informasjonskapsler for sporing, spion- og reklameprogrammer og andre potensielle uønskede programmer. Beskyttelsen rekker lenger enn filene og mappene på din datamaskin, og programmet går etter trusler fra ulike inngangspunkt, inkludert e-post, direktemeldinger og Internett. Krever ingen langtekkelig administrering.

Ressursbevisste søkealternativer

Hvis du opplever lav søkehastighet kan du deaktivere alternativet for minimal bruk av datamaskinressurser, men husk at virusbeskyttelse vil bli høyere prioritert enn andre oppgaver. VirusScan gir deg fleksibilitet til å tilpasse sanntid og manuelle søkealternativer, men selv om du ikke gjør det vil datamaskinen din likevel være beskyttet.

Automatiske reparasjoner

Hvis VirusScan oppdager en sikkerhetstrussel under et sanntids- eller manuelt søk, vil det automatisk forsøke å behandle trusselen etter hvilken type trussel det er. På denne måten kan de fleste trusler oppdager og nøytraliseres uten at du trenger å gjøre noe. Selv om det er sjelden, hender det at VirusScan ikke kan nøytralisere en trussel selv. I slike tilfeller lar VirusScan deg bestemme hva du skal gjøre (søke på nytt neste gang du slår på datamaskinen, beholde det oppdagede elementet eller fjerne det oppdagede elementet).

Midlertidig stans av oppgaver i fullskjermmodus

Når du gjør ting som å se film, spille dataspill eller annen aktivitet som opptar hele dataskjermen, stopper VirusScan midlertidig en rekke oppgaver, inkludert automatiske oppdateringer og manuelle søk.

Starte sanntids virusbeskyttelse

VirusScan tilbyr to typer virusbeskyttelse: sanntid og manuell. Sanntids virusbeskyttelse overvåker konstant datamaskinen for virusaktivitet, og gjennomsøker filer hver gang du eller datamaskinen din bruker dem. Manuell virusbeskyttelse lar deg gjennomsøke filer på kommando. For å forsikre deg om at datamaskinen er beskyttet mot de siste sikkerhetstruslene lar du sanntids virusbeskyttelse være på og lager en tidsplan for faste, mer omfattende manuelle søk. Som standardinnstilling utfører VirusScan et oppsatt søk en gang i uken. For mer informasjon om sanntids- og manuelle søk, se Gjennomsøke datamaskinen (side 57).

Selv om det er sjelden, kan det hende at du ønsker å midlertidig stoppe sanntidssøking (for eksempel for å endre søkealternativer eller utføre feilsøking ang. et ytelsesproblem). Når sanntids virusbeskyttelse er deaktivert, er ikke datamaskinen din beskyttet og beskyttelsesstatusen i SecurityCenter er rød. For mer informasjon om beskyttelsesstatus, se Forstå beskyttelsesstatus i Hjelp for SecurityCenter.

Starte sanntids virusbeskyttelse

Som standardinnstilling er sanntids virusbeskyttelse slått på og beskytter datamaskinen mot virus, trojanske hester og andre sikkerhetstrusler. Hvis du slår av sanntids virusbeskyttelse må du slå den på igjen for å fortsette å være beskyttet.

1 Åpne konfigurasjonsruten for Datamaskin og filer

   Hvordan?

   1. Klikk på **Avansert meny** i den venstre ruten.
   2. Klikk på **Konfigurer**.
   3. Klikk **Datamaskin og filer** i Konfigurer-ruten.

2 Klikk **På** under **Virusbeskyttelse**.

Stoppe sanntids virusbeskyttelse

Du kan slå av sanntids virusbeskyttelse midlertidig og bestemme når den skal starte igjen. Du kan automatisk gjenoppta beskyttelse etter 15, 30, 45 eller 60 minutter, når du slår på datamaskinen igjen eller aldri.

1 Åpne konfigurasjonsruten for Datamaskin og filer

   Hvordan?

1. Klikk på **Avansert meny** i den venstre ruten.
2. Klikk på **Konfigurer**.
3. Klikk **Datamaskin og filer** i Konfigurer-ruten.

2 Klikk **Av** under **Virusbeskyttelse**.

3 I dialogboksen velger du når sanntidssøking skal gjenopptas.

4 Klikk **OK**.

KAPITTEL 9

Starte tilleggsbeskyttelse

I tillegg til sanntids virusbeskyttelse gir VirusScan avansert beskyttelse mot skript, spionprogrammer og potensielt skadelige vedlegg til e-post og direktemeldinger. Som standardinnstilling er skriptsøking, spionprogram-, e-post- og direktemeldingsbeskyttelse slått på og beskytter datamaskinen.

Skriptsøkbeskyttelse

Skriptsøkbeskyttelse oppdager potensielt skadelige skript og hindrer dem i å kjøre på datamaskinen din. Den overvåker datamaskinen for mistenkelig skriptaktivitet, slik som skript som oppretter, kopierer eller sletter filer eller åpner Windows-registret, og varsler deg før det oppstår skade.

Spionprogrambeskyttelse

Spionprogrambeskyttelse oppdager spionprogrammer og andre potensielt uønskede programmer. Spionprogrammer er programvare som installeres på datamaskinen i hemmelighet for å overvåke din atferd, samle inn personlig informasjon og til og med forstyrre din kontroll over datamaskinen ved å installere tilleggsprogramvare eller omdirigere webleseraktivitet.

E-post-beskyttelse

E-post-beskyttelse oppdager mistenkelig aktivitet i e-post og vedlegg du sender og mottar.

Direktemeldingsbeskyttelse

Direktemeldingsbeskyttelse oppdager potensielle sikkerhetstrusler fra direktemeldingsvedlegg du mottar. Den hindrer også direktemeldingsprogrammer i å dele personlig informasjon.

I dette kapitlet

Starte skriptsøkbeskyttelse 36
Starte spionprogrambeskyttelse 36
Starte e-postbeskyttelse.....36
Starte beskyttelse av direktemeldinger.....37

Starte skriptsøkbeskyttelse

Slå på skriptsøkbeskyttelse for å oppdage potensielt skadelige skript og hindre dem i å kjøre på datamaskinen din. Skriptsøkbeskyttelse varsler deg når et skript forsøker å lage, kopiere eller slette filer på datamaskinen eller gjøre endringer i Windows-registret.

1 Åpne konfigurasjonsruten for Datamaskin og filer

Hvordan?

1. Klikk på **Avansert meny** i den venstre ruten.
2. Klikk på **Konfigurer**.
3. Klikk **Datamaskin og filer** i Konfigurer-ruten.

2 Klikk **På** under **Skriptsøkbeskyttelse**.

Merk: Selv om du kan slå av skriptsøkbeskyttelse når som helst, vil det gjøre at datamaskinen er sårbar overfor skadelige skript.

Starte spionprogrambeskyttelse

Slå på spionprogrambeskyttelse for å oppdage og fjerne spion- og reklameprogrammer og andre potensielle uønskede programmer som samler og overfører informasjon uten at du vet det eller har tillat det.

1 Åpne konfigurasjonsruten for Datamaskin og filer

Hvordan?

1. Klikk på **Avansert meny** i den venstre ruten.
2. Klikk på **Konfigurer**.
3. Klikk **Datamaskin og filer** i Konfigurer-ruten.

2 Klikk **På** under **Skriptsøkbeskyttelse**.

Merk: Selv om du kan slå av spionprogrambeskyttelse når som helst, vil det gjøre at datamaskinen er sårbar overfor skadelige skript.

Starte e-postbeskyttelse

Slå på e-post-beskyttelse for å oppdage både ormer og potensielle trusler i utgående (SMTP) og innkommende (POP) e-postmeldinger og vedlegg.

1 Åpne konfigurasjonsruten for E-post og direktemeldinger

Hvordan?

1. Klikk på **Avansert meny** i den venstre ruten.
2. Klikk på **Konfigurer**.
3. Klikk **E-post og direktemeldinger** i ruten Konfigurer.

2 Under **E-postbeskyttelse** klikker du **På**.

Merk: Selv om du kan slå av e-post-beskyttelse når som helst, vil det gjøre at datamaskinen er sårbar overfor e-posttrusler.

Starte beskyttelse av direktemeldinger

Slå på beskyttelse av direktemeldinger for å oppdage sikkerhetstrusler som kan være inkludert i innkommende direktemeldingsvedlegg.

1 Åpne konfigurasjonsruten for E-post og direktemeldinger

Hvordan?

1. Klikk på **Avansert meny** i den venstre ruten.
2. Klikk på **Konfigurer**.
3. Klikk **E-post og direktemeldinger** i ruten Konfigurer.

2 Under **Beskyttelse av direktemeldinger** klikker du **På**.

Merk: Selv om du kan slå av beskyttelse av direktemeldinger når som helst, vil det gjøre at datamaskinen er sårbar overfor skadelige direktemeldingsvedlegg.

KAPITTEL 10

Konfigurere virusbeskyttelse

VirusScan tilbyr to typer virusbeskyttelse: sanntid og manuell. Sanntids virusbeskyttelse gjennomsøker filer hver gang du eller datamaskinen åpner dem. Manuell virusbeskyttelse lar deg gjennomsøke filer på forespørsel. Du kan velge ulike alternativer for hver beskyttelsestype. For eksempel, siden sanntidsbeskyttelse kontinuerlig overvåker datamaskinen, kan du velge et bestemt sett grunnleggende søkealternativer og reservere et mer omfattende sett søkealternativer for manuell beskyttelse på forespørsel.

I dette kapitlet

Konfigurere søkealternativer i sanntid 40
Konfigurere alternativer for manuelt søk 42
Bruke alternativer for SystemGuards.....46
Bruke klarerte lister.....53

Konfigurere søkealternativer i sanntid

Når du starter sanntids virusbeskyttelse bruker VirusScan standardinnstilte alternativer for å gjennomsøke filer; du kan imidlertid endre standardinnstillingene slik at de passer ditt behov.

For å endre sanntids søkealternativer må du bestemme hva VirusScan skal se etter under et søk, samt plasseringen og filtypene det skal gjennomsøke. For eksempel kan du bestemme om VirusScan søker etter ukjente virus eller informasjonskapsler som brukes av webområder til å spore din atferd, og om det skal søke på nettverkstasjoner som er tilordnet datamaskinen din eller bare lokale stasjoner. Du kan også bestemme hva slags type filer som skal gjennomsøkes (alle filer, eller kun programfiler og dokumenter, siden det er der det oppdages flest virus).

Når du endrer sanntids søkealternativer må du også bestemme om det er viktig for datamaskinen å ha beskyttelse mot bufferoverløp. En buffer er en del av minnet som brukes til å midlertidig lagre datainformasjon. Bufferoverløp kan forekomme når mengden informasjon mistenkelige programmer eller prosesser lagrer i en buffer overstiger bufferens kapasitet. Når dette skjer, blir datamaskinen din mer sårbar overfor sikkerhetsangrep.

Konfigurere alternativer for sanntidssøk

Du konfigurerer alternativer for sanntidssøk for å tilpasse hva VirusScan søker etter under et sanntidssøk, samt plasseringene og filtypene det gjennomsøker. Alternativer inkluderer å søke etter ukjente virus og informasjonskapsler for sporing, samt beskytte mot bufferoverløp. Du kan også konfigurere sanntidssøk til å gjennomsøke nettverksstasjoner som er tilordnet datamaskinen din.

1 Åpne ruten for Sanntidssøk.

Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. Klikk **Datamaskin og filer** i Hjem-ruten i SecurityCenter.
3. I informasjonsdelen for Datamaskin og filer klikker du **Konfigurer**.
4. Kontroller at virusbeskyttelse er aktivert i ruten for Datamaskin og filer, og klikk deretter **Avansert**.

2 Spesifiser alternativene for sanntidssøk og klikk deretter **OK**.

For å...	Gjør dette ...
Oppdag ukjente virus og nye varianter av kjente virus	Merk av i boksen for **Søk etter ukjente virus som bruker heuristikk**.
Oppdag informasjonskapsler	Merk av i boksen for **Søk etter og fjern informasjonskapsler for sporing**.
Oppdag virus og andre potensielle trusler på stasjoner som er tilkoblet nettverket ditt	Merk av i boksen **Søk gjennom nettverksstasjoner**.
Beskytt datamaskinen mot bufferoverløp	Merk av i boksen for **Aktiver beskyttelse mot bufferoverløp**.
Angi hvilke typer filer som skal gjennomsøkes:	Klikk enten **Alle filer (anbefales)** eller **Bare programfiler og dokumenter**.

Konfigurere alternativer for manuelt søk

Manuell virusbeskyttelse lar deg gjennomsøke filer på forespørsel. Når du starter et manuelt søk, gjennomsøker VirusScan datamaskinen din for virus og andre potensielle skadelige elementer ved å bruke et mer omfattende sett søkealternativer. For å endre manuelle søkealternativer må du bestemme hva VirusScan skal søke etter under et søk. For eksempel kan du bestemme om VirusScan skal se etter ukjente virus, potensielle uønskede programmer som f.eks. spion- eller reklameprogrammer, skjulte programmer som f.eks. rootkits som kan gi uautorisert tilgang til datamaskinen, og informasjonskapsler som webområder kan bruke til å spore atferden din. Du må også bestemme hvilke typer filer som skal gjennomsøkes. For eksempel kan du bestemme om VirusScan skal gjennomsøke alle filer eller bare programfiler og dokumenter (siden det er her det oppdages flest virus). Du kan også bestemme om komprimerte filer (f.eks. .zip-filer) skal inkluderes i søket.

Som standardinnstilling gjennomsøker VirusScan alle stasjoner og mapper på datamaskinen hver gang det kjører et manuelt søk; du kan imidlertid endre standardinnstillingene slik at de passer til ditt behov. For eksempel kan du gjennomsøke bare kritiske systemfiler, elementer på skrivebordet eller elementer i mappen for Programfiler. Hvis du ikke vil ha ansvaret for å starte hvert manuelle søk selv, kan du lage en fast tidsplan for søk. Oppsatte søk gjennomsøker alltid hele datamaskinen ved å bruke standardinnstillingene for søk. Som standardinnstilling utfører VirusScan et oppsatt søk en gang i uken.

Hvis du opplever lav søkehastighet kan du deaktivere alternativet for minimal bruk av datamaskinressurser, men husk at virusbeskyttelse vil bli høyere prioritert enn andre oppgaver.

Merk: Når du gjør ting som å se film, spille dataspill eller annen aktivitet som opptar hele dataskjermen, stopper VirusScan midlertidig en rekke oppgaver, inkludert automatiske oppdateringer og manuelle søk.

Konfigurere alternativer for manuelt søk

Du konfigurerer alternativer for manuelt søk for å tilpasse hva VirusScan søker etter under et manuelt søk, samt plasseringene og filtypene det gjennomsøker. Alternativer inkluderer søk etter ukjente virus, komprimerte filer, spionprogrammer og potensielt uønskede programmer, informasjonskapsler for sporing, rootkits og skjulte programmer.

1 Åpne ruten for Manuelt søk.

Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. Klikk **Datamaskin og filer** i Hjem-ruten i SecurityCenter.
3. I informasjonsdelen for Datamaskin og filer klikker du **Konfigurer**.
4. Kontroller at virusbeskyttelse er aktivert i ruten for Datamaskin og filer, og klikk deretter **Avansert**.
5. Klikk på **Manuelt søk** i ruten Virusbeskyttelse.

2 Spesifiser alternativene for manuelt søk og klikk deretter **OK**.

For å...	Gjør dette ...
Oppdage ukjente virus og nye varianter av kjente virus	Merk av i boksen for **Søk etter ukjente virus som bruker heuristikk**.
Oppdage og fjerne virus i ZIP-filer og andre komprimerte filer.	Merk av i boksen for **Søk i ZIP-filer og andre komprimerte filer**.
Oppdage spion- og reklameprogrammer og andre potensielle uønskede programmer.	Merk av i boksen for **Søk etter spionprogrammer og potensielt uønskede programmer**.
Oppdage informasjonskapsler	Merk av i boksen for **Søk etter og fjern informasjonskapsler for sporing**.
Oppdage rootkits og skjulte programmer som kan endre og utnytte eksisterende systemfiler for Windows	Merk av i boksen for **Søk etter rootkits og andre skjulte programmer**.
Bruke mindre prossessorkraft for søk og prioriter andre oppgaver høyere (som f.eks. weblesing eller åpning av dokumenter)	Merk av i boksen for **Søk med minimale datamaskinressurser**.
Angi hvilke typer filer som skal gjennomsøkes	Klikk enten **Alle filer (anbefales)** eller **Bare programfiler og dokumenter**.

Konfigurere plassering for manuelt søk

Du konfigurerer plasseringen for manuelt søk for å bestemme hvor VirusScan skal søke etter virus og andre skadelige elementer under et manuelt søk. Du kan gjennomsøke alle filer, mapper og stasjoner på datamaskinen eller du kan begrense søket til bestemte mapper og stasjoner.

1 Åpne ruten for Manuelt søk.

Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. Klikk **Datamaskin og filer** i Hjem-ruten i SecurityCenter.
3. I informasjonsdelen for Datamaskin og filer klikker du **Konfigurer**.
4. Kontroller at virusbeskyttelse er aktivert i ruten for Datamaskin og filer, og klikk deretter **Avansert**.
5. Klikk på **Manuelt søk** i ruten Virusbeskyttelse.

2 Klikk på **Standard plassering som skal gjennomsøkes**.

3 Spesifiser plasseringen for manuelt søk og klikk deretter **OK**.

For å...	Gjør dette ...
Gjennomsøke aller filer og mapper på datamaskinen	Merk av i boksen for **(Min) Datamaskin**.
Gjennomsøke bestemte filer, mapper og stasjoner på datamaskinen	Fjern merket i boksen for **(Min) Datamaskin** og velg en eller flere mapper eller stasjoner.
Gjennomsøke kritiske systemfiler	Fjern merket i boksen for **(Min) Datamaskin** og merk deretter av i boksen for **Kritiske systemfiler**.

Planlegge et søk

Planlegg søk for å gjennomføre et grundig søk av datamaskinen etter virus og andre trusler hvilken som helst dag og tidspunkt i uken. Planlagte søk gjennomsøker alltid hele datamaskinen ved å bruke standardinnstillingene for søk. Som standardinnstilling utfører VirusScan et planlagt søk en gang i uken. Hvis du opplever lav søkehastighet kan du deaktivere alternativet for minimal bruk av datamaskinressurser, men husk at virusbeskyttelse vil bli høyere prioritert enn andre oppgaver.

1 Åpne ruten for Planlagt søk.

Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. Klikk **Datamaskin og filer** i Hjem-ruten i SecurityCenter.
3. I informasjonsdelen for Datamaskin og filer klikker du **Konfigurer**.
4. Kontroller at virusbeskyttelse er aktivert i ruten for Datamaskin og filer, og klikk deretter **Avansert**.
5. Klikk på **Planlagt søk** i ruten Virusbeskyttelse.

2 Velg **Aktiver planlagt søk**.

3 For å redusere mengden prosessorkraft som vanligvis brukes til søking velger du **Utfør søk med minimal bruk av datamaskinressurser**.

4 Velg en eller flere dager.

5 Spesifiser starttidspunkt.

6 Klikk **OK**.

Tips: Du kan gjenopprette standardtidsplanen ved å klikke **Tilbakestill**.

Bruke alternativer for SystemGuards

Systemguards overvåker, logger, rapporterer og administrerer potensielle uautoriserte endringer som er gjort i Windows-registret eller kritiske systemfiler på datamaskinen. Uautoriserte endringer i register og filer kans kade datamaskinen, sette sikkerheten på spill og skade verdifulle systemfiler.

Endringer i register og filer er vanlig og oppstår regelmessig på datamaskinen. Siden mange er uskadelige, er SystemGuards' standardinnstillinger konfigurert til å sørge for pålitelig, intelligent og ekte beskyttelse mot uautoriserte endringer som kan være skadelige. For eksempel, når SystemGuards oppdager uvanlige endringer som kan være en mulig trussel, blir aktiviteten øyeblikkelig rapportert og registrert. Mer vanlige endringer som likevel kan være en trussel, blir kun registrert. Som standardinnstilling er imidlertid overvåking av standardendringer og endringer med lav risiko deaktivert. SystemGuards-teknologien kan konfigureres til å utvide beskyttelsen til et hvilket som helst miljø.

Det finnes tre typer SystemGuards: SystemGuards for programmer, SystemGuards for Windows og SystemGuards for webleser.

SystemGuards for programmer

SystemGuards for programmer oppdager potensielle uautoriserte endringer i datamaskinens register og andre kritiske filer som er viktige for Windows. Disse viktige registerelementene og filene er bl.a. ActiveX-installasjoner, oppstartselementer, shell execute hooks i Windows og shell service object delay loads. Ved å overvåke disse stopper SystemGuards for programmer mistenkelige ActiveX-programmer (nedlastet fra Internett) i tillegg til spionprogrammer og potensielle uønskede programmer som kan starte automatisk når Windows starter.

SystemGuards for Windows

SystemGuards for Windows oppdager også potensielle uautoriserte endringer i datamaskinens register og andre kritiske filer som er viktige for Windows. Disse viktige registerelementene og filene er bl.a. hurtigmenystyring, appInit DLLs og Windows Hosts-filen. Ved å overvåke disse hjelper SystemGuards for Windows til med å hindre at datamaskinen din sender og mottar uautorisert eller personlig informasjon over Internett. Det hjelper også til med å stoppe programmer som kan komme med uventede endringer i utseendet og atferden til programmer som er viktige for deg og din familie.

SystemGuards for webleser

Akkurat som SystemGuards for programmer og Windows oppdager også SystemGuards for webleser potensielle uautoriserte endringer i datamaskinens register og andre kritiske filer som er viktige for Windows. SystemGuards for webleser overvåker derimot endringer i viktige registerelementer og filer som f.eks. Internet Explorer-tillegg, Internet Explorer URL-er og Internett Explorer sikkerhetssoner. Ved å overvåke disse, hjelper SystemGuards for webleser til med å hindre uautorisert webleseraktivitet, som f.eks. videresending til mistenkelige webområder, endringer i innstillinger og alternativer for webleser uten at du vet om det, og uønsket klarering av mistenkelige webområder.

Aktivere SystemGuards-beskyttelse

Aktiver SystemGuards-beskyttelse for å oppdage og bli varslet om potensielle uautoriserte endringer i Windows-register og filer på datamaskinen. Uautoriserte endringer i register og filer kan skade datamaskinen, sette sikkerheten på spill og skade verdifulle systemfiler.

1 Åpne konfigurasjonsruten for Datamaskin og filer

Hvordan?

1. Klikk på **Avansert meny** i den venstre ruten.
2. Klikk på **Konfigurer**.
3. Klikk **Datamaskin og filer** i Konfigurer-ruten.

2 Klikk **På** under **SystemGuard-beskyttelse**.

Merknad: Du kan deaktivere SystemGuard-beskyttelse ved å klikke på **Av**.

Konfigurere alternativer for SystemGuards

Bruk ruten SystemGuards for å konfigurere beskyttelses-, logging- og varslingsalternativer mot uautoriserte register- og filendringer tilknyttet Windows-filer og -programmer og Internett Explorer. Uautoriserte endringer i register og filer kan skade datamaskinen, sette sikkerheten på spill og skade verdifulle systemfiler.

1 Åpne ruten SystemGuards.

   Hvordan?

   1. Under **Vanlige oppgaver** klikker du **Hjem**.
   2. Klikk **Datamaskin og filer** i Hjem-ruten i SecurityCenter.
   3. I informasjonsdelen for Datamaskin og filer klikker du **Konfigurer**.
   4. Kontroller at SystemGuard-beskyttelse er aktivert i ruten for Datamaskin og filer, og klikk deretter **Avansert**.

2 Velg en SystemGuards-type fra listen.

   - **SystemGuards for programmer**
   - **SystemGuards for Windows**
   - **SystemGuards for webleser**

3 Under **Jeg vil** gjør du ett av følgende:

   - Hvis du vil oppdage, logge og rapportere uautoriserte register- og filendringer tilknyttet SystemGuards for programmer, Windows og webleser, klikker du på **Vis varsler.**
   - Hvis du vil oppdage og logge uautoriserte register- og filendringer tilknyttet SystemGuards for programmer, Windows og webleser, klikker du på **Bare logg endringer.**
   - Hvis du vil deaktivere oppdaging av uautoriserte register- og filendringer tilknyttet SystemGuards for programmer, Windows og webleser, klikker du på **Deaktiver SystemGuard.**

Merk: For mer informasjon om SystemGuards-typer, se Om SystemGuards-typer (side 49).

Om SystemGuards-typer

SystemGuards oppdager potensielle uautoriserte endringer i datamaskinens register og andre kritiske filer som er viktige for Windows. Det finnes tre typer SystemGuards: SystemGuards for programmer, SystemGuards for Windows og SystemGuards for webleser.

SystemGuards for programmer

SystemGuards for programmer stopper mistenkelige ActiveX-programmer (nedlastet fra Internett) i tillegg til spionprogrammer og potensielle uønskede programmer som kan starte automatisk når Windows starter.

SystemGuard	Oppdager...
ActiveX-installasjoner	Uautoriserte registerendringer i ActiveX-installasjoner som kan skade datamaskinen, sette sikkerheten på spill og skade verdifulle systemfiler.
Oppstartselementer	Spion- og reklameprogrammer og andre potensielle uønskede programmer som kan installere filendringer i oppstartselementer og lar mistenkelige programmer kjøre når du starter datamaskinen.
Shell Execute Hooks i Windows	Spion- og reklameprogrammer eller andre potensielt uønskede programmer som kan installere shell execute hooks for å hindre at sikkerhetsprogrammer kjøres.
Shell Service Object Delay Load	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape registerendringer i shell service object delay load og la skadelige filer kjøre når du starter datamaskinen.

SystemGuards for Windows

SystemGuards for Windows hjelper til med å hindre at datamaskinen din sender og mottar uautorisert eller personlig informasjon over Internett. Det hjelper også til med å stoppe programmer som kan komme med uventede endringer i utseendet og atferden til programmer som er viktige for deg og din familie.

SystemGuard	Oppdager...
Hurtigmenystyring	Uautoriserte registerendringer i Windows hurtigmenystyring som kan påvirke utseendet og atferden til Windows-menyer. Hurtigmenyer lar deg utføre handlinger på datamaskinen, som f.eks. å høyreklikke filer.

AppInit DLLs	Uautoriserte registerendringer i Windows appInit DLLs som kan tillate potensielt skadelige filer å kjøre når du starter datamaskinen.
Windows Hosts-fil	Spion- og reklameprogrammer og potensielt uønskede programmer som kan skape uautoriserte endringer i Windows hosts-filen, tillate webleseren å omdirigeres til mistenkelige webområder og blokkere programoppdateringer.
Winlogon-skall	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape registerendringer i Winlogon-skallet og tillate andre programmer å erstatte Windows Utforsker.
Winlogon User Init	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape registerendringer i Winlogon user init og lar mistenkelige programmer kjøre når du logger på Windows.
Windows-protokoller	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape registerendringer i Windows-protokoller og påvirke måten datamaskinen sender og mottar informasjon over Internett på.
Winsock Layered Service Providers	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan installere registerendringer i Winsock Layered Service Providers (LSPs) for å fange opp og endre informasjon du sender og mottar over Internett.
Windows Shell Open Commands	Uautoriserte endringer i Windows shell open commands som kan tillate ormer og andre skadelige programmer å kjøre på datamaskinen.
Shared Task Scheduler	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape register- og filendringer i shared task scheduler og la potensielt skadelige filer kjøre når du starter datamaskinen.
Windows Messenger-tjenesten	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape registerendringer i Windows Messenger-tjenesten og tillate uønskede reklamer og kjøre eksterne programmer på datamaskinen.
Windows Win.ini-fil	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape endringer i Win.ini-filen og la mistenkelige programmer kjøre når du starter datamaskinen.

SystemGuards for webleser

SystemGuards for webleser hjelper til med å hindre uautorisert webleseraktivitet, som f.eks. videresending til mistenkelige webområder, endringer i innstillinger og alternativer for webleser uten at du vet om det, og uønsket klarering av mistenkelige webområder.

SystemGuard	Oppdager...
Hjelpeobjekter for weblesere	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan bruke hjelpeobjekter for webleser til å spore weblesing og vise uønsket reklame.
Internet Explorer-verktøylinjer	Uautoriserte registerendringer i programmer for Internet Explorer-verktøylinjer, som f.eks. Søk og Favoritter, som kan påvirke utseendet og atferden til Internet Explorer.
Tillegg for Internet Explorer	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan installere tillegg for Internet Explorer til å spore weblesing og vise uønsket reklame.
Internet Explorer ShellBrowser	Uautoriserte registerendringer i Internet Explorer shell browser som kan påvirke utseendet og atferden til webleseren.
Internet Explorer WebBrowser	Uautoriserte registerendringer i Internet Explorer Webleser som kan påvirke utseendet og atferden til webleseren.
Internet Explorer-bindinger for URL-søk	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape registerendringer i Internet Explorer-bindinger for URL-søk og tillate webleseren å bli omdirigert til mistenkelige webområder når du søker på nettet.
Internet Explorer-URLer	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape registerendringer i Internet Explorer URL-er og påvirke innstillingene for webleseren.
Internet Explorer-begrensninger	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape registerendringer i Internet Explorer URL-er og påvirke innstillingene og alternativene for webleseren.
Sikkerhetssoner i Internet Explorer	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape registerendringer i sikkerhetssoner i Internet Explorer og la potensielt skadelige filer kjøre når du starter datamaskinen.

Klarerte områder i Internet Explorer	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape registerendringer i klarerte områder i Internet Explorer og tillate webleseren å klarere mistenkelige webområder.
Internet Explorer-policy	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape registerendringer i Internet Explorer-policyer og påvirke utseendet og atferden til webleseren.

Bruke klarerte lister

Hvis VirusScan oppdager endringer i filer eller register (SystemGuard), program eller bufferoverløp, blir du bedt om å klarere eller fjerne det. Hvis du klarerer elementet og sier at du ikke vil motta flere meldinger om elementets aktivitet, blir elementet lagt til i en klarert liste og VirusScan vil ikke lenger oppdage det eller melde fra om aktiviteten til det. Hvis et element har blitt lagt til i en klarert liste, men du ønsker å blokkere aktiviteten, kan du gjøre det. Å blokkere hindrer elementet fra å kjøre eller foreta endringer på datamaskinen uten å melde fra hver gang det blir gjort et forsøk. Du kan også fjerne et element fra en klarert liste. Å fjerne et element gjør at VirusScan kan oppdage elementets aktivitet igjen.

Behandle klarerte lister

Bruk ruten Klarerte lister for å klarere eller blokkere elementer som tidligere har blitt oppdaget og klarert. Du kan også fjerne et element fra en klarert liste slik at VirusScan kan oppdage det igjen.

1 Åpne ruten Klarerte lister

Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. Klikk **Datamaskin og filer** i Hjem-ruten i SecurityCenter.
3. I informasjonsdelen for Datamaskin og filer klikker du **Konfigurer**.
4. Kontroller at virusbeskyttelse er aktivert i ruten for Datamaskin og filer, og klikk deretter **Avansert**.
5. Klikk på **Klarerte lister** i ruten Virusbeskyttelse.

2 Velg en av følgende typer klarerte lister:

- **SystemGuards for programmer**
- **SystemGuards for Windows**
- **SystemGuards for webleser**
- **Klarerte programmer**
- **Klarerte bufferoverløp**

3 Under **Jeg vil** gjør du ett av følgende:

- Hvis du vil tillate det oppdagede elementet å foreta endringer i Windows-registret eller kritiske systemfiler på datamaskinen uten å melde fra, klikker du på **Klarer**.
- Hvis du vil blokkere det oppdagede elementet fra å foreta endringer i Windows-registret eller kritiske systemfiler på datamaskinen uten å melde fra, klikker du på **Blokker**.

- For å fjerne det oppdagede elementet fra klarerte lister, klikker du på **Fjern**.

4 Klikk **OK**.

Merk: For mer informasjon om typer av klarerte lister, se Om typer av klarerte lister (side 54).

Om typer av klarerte lister

SystemGuards i ruten Klarerte lister viser tidligere uautoriserte register- og filendringer som VirusScan har oppdaget, men som du kan ha valgt å tillate fra et varsel eller fra ruten Søkeresultater. Det finnes fem typer klarerte lister som du kan administrere i ruten Klarerte lister: SystemGuards for programmer, SystemGuards for Windows, SystemGuards for webleser, Klarerte programmer og Klarerte bufferoverløp.

Alternativer	Beskrivelse
SystemGuards for programmer	SystemGuards for programmer i ruten Klarerte lister viser tidligere uautoriserte register- og filendringer som VirusScan har oppdaget, men som du kan ha valgt å tillate fra et varsel eller fra ruten Søkeresultater. SystemGuards for programmer oppdager uautoriserte register- og filendringer tilknyttet ActiveX-installasjoner, oppstartselementer, shell execute hooks i Windows og aktivitet i shell service object delay load. Slike typer uautoriserte endringer i register og filer kan skade datamaskinen, sette sikkerheten på spill og skade verdifulle systemfiler.
SystemGuards for Windows	SystemGuards for programmer i ruten Klarerte lister viser tidligere uautoriserte register- og filendringer som VirusScan har oppdaget, men som du kan ha valgt å tillate fra et varsel eller fra ruten Søkeresultater. SystemGuards for Windows oppdager uautoriserte register- og filendringer tilknyttet hurtigmenystyring, appInit DLLs, Windows hosts-filen, Winlogon-skallet, Winsock Layered Service Providers (LSPs) osv. Slike typer uautoriserte register- og filendringer kan påvirke måten datamaskinen sender og mottar informasjon over Internett på, endre utseendet og atferden til programmer og tillate mistenkelige programmer å kjøre på datamaskinen.

SystemGuards for webleser	SystemGuards for webleser i ruten Klarerte lister viser tidligere uautoriserte register- og filendringer som VirusScan har oppdaget, men som du kan ha valgt å tillate fra et varsel eller fra ruten Søkeresultater. SystemGuards for webleser oppdager uautoriserte registerendringer og annen uønsket atferd tilknyttet hjelpeobjekter for weblesere, Internet Explorer-tillegg, Internet Explorer URL-er, sikkerhetssoner i Internet Explorer osv. Slike typer uautoriserte registerendringer kan resultere i uønsket webleseraktivitet, slik som omdirigering til mistenkelige webområder, endringer i webleserens innstillinger og alternativer og klarering av mistenkelige webområder.
Klarerte programmer	Klarerte programmer er potensielt uønskede programmer som VirusScan tidligere har oppdaget, men som du har valgt å klarere fra et varsel eller fra ruten Søkeresultater.
Klarerte bufferoverløp	Klarerte bufferoverløp er potensielt uønsket aktivitet som VirusScan tidligere har oppdaget, men som du har valgt å klarere fra et varsel eller fra ruten Søkeresultater. Bufferoverløp kan skade datamaskinen og ødelegge filer. Bufferoverløp forekommer når mengden informasjon mistenkelige programmer eller prosesser lagrer i en buffer overstiger bufferens kapasitet.

KAPITTEL 11

Gjennomsøke datamaskinen

Når du starter SecurityCenter første gang, begynner sanntids virusbeskyttelsen i VirusScan å beskytte datamaskinen mot potensielt skadelige virus, trojanske hester og andre sikkerhetstrusler. Dersom du ikke deaktiverer sanntids virusbeskyttelse, vil VirusScan kontinuerlig overvåke datamaskinen for virusaktivitet og gjennomsøke filer hver gang du eller datamaskinen åpner dem ved å bruke alternativene for sanntidssøk som du har valgt. For å forsikre deg om at datamaskinen er beskyttet mot de siste sikkerhetstruslene lar du sanntids virusbeskyttelse være på og lager en tidsplan for faste, mer omfattende manuelle søk. For mer informasjon om innstilling av sanntids- og manuelle søkealternativer kan du se Konfigurere virusbeskyttelse (side 39).

VirusScan tilbyr et detaljert sett søkealternativer for manuell virusbeskyttelse, som lar deg utføre mer omfattende søk regelmessig. Du kan utføre manuelle søk fra SecurityCenter i bestemte plasseringer etter en oppsatt tidsplan. Du kan imidlertid også utføre manuelle søk direkte i Windows Utforsker mens du arbeider. Søking i SecurityCenter har den fordelen at du kan endre søkealternativer i full fart. Søking fra Windows Utforsker tilbyr imidlertid en praktisk tilnærming til datasikkerhet.

Uansett om du utfører manuelt søk fra SecurityCenter eller Windows Utforsker kan du se søkeresultatene når søket er ferdig. Du kan bruke søkeresultatenefor å se om VirusScan har oppdaget, reparert eller isolert virus, trojanske hester, spion- og reklameprogrammer, informasjonskapsler og andre potensielt uønskede programmer. Søkeresultatene kan vises på flere måter. Du kan for eksempel se et sammendrag av søkeresultatene eller detaljert informasjon, som f.eks. infeksjonens status og type. Du kan også se generell statistikk for søk og oppdagelser.

I dette kapitlet

Gjennomsøke datamaskinen 58
Vise søkeresultater 58

Gjennomsøke datamaskinen

Du kan utføre et manuelt søk fra enten Avansert eller Grunnleggende meny i SecurityCenter. Hvis du utfører søk fra Avansert meny kan du bekrefte alternativene for manuelt søk før du søker. Hvis du utfører søk fra Grunnleggende meny starter VirusScan søket øyeblikkelig ved å bruke de eksisterende søkealternativene. Du kan også utføre søk i Windows Utforsker med de eksisterende søkealternativene.

- Gjør ett av følgende:

  Søk i SecurityCenter

For å...	Gjør dette ...
Søk med eksisterende innstilliger	Klikk på **Søk** i Grunnleggende meny.
Søk med endrede innstilliger	Klikk **Søk** i Avansert meny, velg hvilke plasseringer som skal gjennomsøkes, velg søkealternativer og klikk deretter på **Søk nå**.

  Søke i Windows Utforsker

  1. Åpne Windows Utforsker.
  2. Høyreklikk på en fil, mappe eller stasjon og klikk deretter på **Søk**.

Merknad: Søkeresultatene vises i varslet for Søk fullført. Resultatene består av antallet gjennomsøkte, oppdagede, reparerte, ignorerte og fjernede elementer. Klikk på **Vis søkedetaljer** for å lese mer om søkeresultatene eller arbeide med infiserte elementer.

Vise søkeresultater

Når et manuelt søk er ferdig kan du vise resultatene for å se hva søket fant og for å analysere datamaskinens gjeldende beskyttelsesstatus. Søkeresultatene forteller deg om VirusScan har oppdaget, reparert eller isolert virus, trojanske hester, spion- og reklameprogrammer, informasjonskapsler og andre potensielt uønskede programmer.

- I Grunnleggende eller Avansert meny klikker du på **Søk** og gjør så ett av følgende:

For å...	Gjør dette ...
Vise søkeresultater i varslet	Vise søkeresultater i varslet for Søk fullført.
Vise mer informasjon om søkeresultater	Klikk på **Vis søkedetaljer** i varslet for Søk fullført.

Vise et kort sammendrag av søkeresultatene	Pek på **Ikonet for Søk fullført** i informasjonsdelen på oppgavelinjen.
Vise statistikk for søk og oppdagelse	Dobbelklikk **Søk fullført**-ikonet i informasjonsdelen på oppgavelinjen.
Vise detaljer om oppdagede elementer, infeksjonsstatus og -type.	Dobbelklikk **Søk fullført**-ikonet i informasjonsdelen på oppgavelinjen, og klikk deretter på **Vis resultater** i Søkeframdrift: Ruten Manuelt søk.

KAPITTEL 12

Arbeide med søkeresultater

Hvis VirusScan oppdager en sikkerhetstrussel under et sanntids- eller manuelt søk, vil det automatisk forsøke å behandle trusselen etter hvilken type trussel det er. Hvis VirusScan for eksempel oppdager et virus, trojansk hest eller informasjonskapsel for sporing på datamaskinen, forsøker det å rense den infiserte filen. Hvis filen ikke kan renses, isolerer VirusScan den.

Noen sikkerhetstrusler kan det hende VirusScan ikke kan rense eller isolere. Hvis dette skjer, vil VirusScan be deg om å behandle trusselen. Du kan foreta ulike handlinger avhengig av typen trussel. Hvis for eksempel et virus blir oppdaget i en fil, og VirusScan ikke kan rense eller isolere filen, nekter den adgang til filen. Hvis informasjonskapsler for sporing blir oppdaget, og VirusScan ikke kan rense eller isolere informasjonskapslene, kan du bestemme om de skal fjernes eller klareres. Hvis potensielt uønskede programmer blir oppdaget foretar ikke VirusScan seg noe umiddelbart, i stedet lar det deg bestemme om programmet skal isoleres eller klareres.

Når VirusScan isolerer elementer, krypterer og isolerer det elementene i en mappe for å hindre filene, programmene eller informasjonskapslene i å skade datamaskinen. Du kan gjenopprette eller fjerne de isolerte elementene. I de fleste tilfeller kan du slette en isolert informasjonskapsel uten å påvirke systemet; hvis VirusScan derimot har isolert et program du gjenkjenner og bruker, bør du vurdere å gjenopprette det.

I dette kapitlet

Arbeide med virus og trojanske hester 61
Arbeide med potensielt uønskede programmer.....62
Arbeide med isolerte filer 62
Arbeide med isolerte programmer og informasjonskapsler 63

Arbeide med virus og trojanske hester

Hvis VirusScan oppdager et virus eller en trojansk hest i en fil på datamaskinen under et sanntids eller manuelt søk, forsøker det å rense filen. Hvis filen ikke kan renses, forsøker VirusScan å isolere den. Hvis dette heller ikke går, nektes det adgang til filen (kun i sanntidssøk).

1 Åpne ruten Søkeresultater.

Hvordan?

1. Dobbelklikk **Søk fullført**-ikonet i informasjonsdelen helt til høyre på oppgavelinjen.
2. I Søkeframdrift: Ruten Manuelt søk, klikk på **Vis resultater**.

2 I listen over søkeresultater klikker du på **Virus og trojanske hester**.

Merknad: Hvis du vil arbeide med filene VirusScan har isolert, se Arbeide med isolerte filer (side 62).

Arbeide med potensielt uønskede programmer

Hvis VirusScan oppdager et potensielt uønsket program på datamaskinen under et sanntids- eller manuelt søk, kan du enten fjerne eller klarere programmet. Å fjerne et potensielt uønsket program sletter det ikke fra systemet. I stedet isoleres programmet for å hindre at det skader datamaskinen eller filer.

1 Åpne ruten Søkeresultater.

Hvordan?

1. Dobbelklikk **Søk fullført**-ikonet i informasjonsdelen helt til høyre på oppgavelinjen.
2. I Søkeframdrift: Ruten Manuelt søk, klikk på **Vis resultater**.

2 I listen over søkeresultater klikker du på **Potensielt uønskede programmer.**

3 Velg et potensielt uønsket program.

4 Under **Jeg vil** klikker du enten **Fjern** eller **Klarer**.

5 Bekreft valget.

Arbeide med isolerte filer

Når VirusScan isolerer infiserte filer, krypterer og flytter det filene til en mappe for å hindre dem i å skade datamaskinen. Du kan deretter gjenopprette eller fjerne de isolerte elementene.

1 Åpne ruten Isolerte filer.

Hvordan?

1. Klikk på **Avansert meny** i den venstre ruten.
2. Klikk på **Gjenopprett**.
3. Klikk på **Filer**.

2 Velg en isolert fil.

3 Gjør ett av følgende:

- Hvis du vil reparere den infiserte filen og flytte den tilbake til sin opprinnelige plassering på datamaskinen, klikker du **Gjenopprett**.
- Hvis du vil fjerne den infiserte filen fra datamaskinen klikker du **Fjern**.

4 Klikk **Ja** for å bekrefte valget.

Tips: Du kan gjenopprette eller fjerne flere filer samtidig.

Arbeide med isolerte programmer og informasjonskapsler

Når VirusScan isolerer potensielt uønskede programmer eller informasjonskapsler for sporing, krypterer og flytter det dem til en beskyttet mappe for å hindre programmene eller informasjonskapslene i å skade datamaskinen. Du kan gjenopprette eller fjerne de isolerte elementene. I de fleste tilfeller kan du slette et isolert element uten at det påvirker systemet.

1 Åpne ruten Isolerte programmer og informasjonskapsler for sporing.

Hvordan?

1. Klikk på **Avansert meny** i den venstre ruten.
2. Klikk på **Gjenopprett**.
3. Klikk på **Programmer og informasjonskapsler**.

2 Velg et isolert program eller informasjonskapsel.

3 Gjør ett av følgende:

- Hvis du vil reparere den infiserte filen og flytte den tilbake til sin opprinnelige plassering på datamaskinen, klikker du **Gjenopprett**.
- Hvis du vil fjerne den infiserte filen fra datamaskinen klikker du **Fjern**.

4 Klikk **Ja** for å bekrefte handlingen.

Tips: Du kan gjenopprette eller fjerne flere programmer og informasjonskapsler samtidig.

KAPITTEL 13

McAfee Personal Firewall

Personal Firewall gir avansert beskyttelse til datamaskinen og dine personlige opplysninger. Personal Firewall oppretter en barriere mellom datamaskinen og Internett og overvåker all Internett-trafikk i bakgrunnen.

Merknad: SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer så snart det oppdager dem. Hvis du trenger hjelp til å diagnostisere beskyttelsesproblemene, kan du kjøre McAfee Virtual Technician.

I dette kapitlet

Personal Firewall-funksjoner 66
Starte Firewall 69
Arbeide med varsler 71
Håndtere informasjonsvarsler 75
Konfigurere Firewall-beskyttelse 77
Administrere programmer og tillatelser 89
Behandle systemtjenester 97
Administrere datamaskintilkoblinger 103
Logge, overvåke og analysere 111
Lære om Internett-sikkerhet 121

Personal Firewall-funksjoner

Personal Firewall har følgende funksjoner.

Standard og egendefinert beskyttelsesnivå

Beskyttelse mot inntrenging og mistenkelig aktivitet ved å bruke Firewalls standard egendefinerte beskyttelsesinnstillinger

Anbefalinger i sanntid

Motta dynamiske anbefalinger som hjelper deg å bestemme om programmer skal få Internett-tilgang eller om du kan stole på nettverkstrafikk.

Intelligent tilgangsadministrasjon for programmer

Håndter Internett-tilgang via varsler og hendelseslogg, eller konfigurere tilgangstillatelser for spesifikke programmer.

Spillebeskyttelse

Forhindrer at varsler om inntrengingsforsøk og mistenkelige aktiviteter distraherer deg mens du spiller i fullskjermmodus.

Beskyttelse ved oppstart

Så snart Windows® starter, beskytter Firewall datamaskinen din fra inntrengingsforsøk og uønskede programmer og nettverkstrafikk.

Kontroll av systemtjenesteport

Administrerer åpne og lukkede systemtjenesteporter som kreves av visse programmer.

Administrerer datamaskintilkoblinger

Tillate og blokkere eksterne tilkoblinger mellom andre datamaskiner og din datamaskin.

Integrasjon av HackerWatch-informasjon

Sporer global hacking- og inntrengingsmønstre via HackerWatch's webområde, som også gir oppdatert sikkerhetsinformasjon om programmer på datamaskinen din og statistikk om globale sikkerhetshendelser og Internett-port.

Sperr brannmur

Blokkerer øyeblikkelig all innkommende og utgående trafikk mellom datamaskinen og Internett.

Gjenopprette Firewall

Gjenoppretter øyeblikkelig Firewalls originale beskyttelsesinnstillinger.

Avanserte funksjoner for oppdagelse av trojanske hester

Oppdager og blokkere potensielle skadelige programmer, som for eksempel trojanske hester, fra å videresende dine personlige opplysninger over Internett.

Hendelseslogging

Sporer nylig innkommende, utgående og inntrengingshendelser.

Overvåke Internett-trafikk

Gå gjennom kart som viser kilden til aggressive angrep og aggressiv trafikk over hele verden. I tillegg kan du få detaljert eierinformasjon og geografiske data om de opprinnelige IP-adressene. Analyserer også innkommende og utgående trafikk og overvåker programbåndbredde og programaktivitet.

Inntrengingshindring

Beskytter ditt personvern fra mulige Internett-trusler. Ved hjelp av heuristisklignende funksjonalitet tilbyr McAfee et tertiært beskyttelseslag som blokkerer elementer som viser tegn på angrep eller de samme karakteristikkene som hackerangrep.

Avansert trafikkanalyse

Gjennomgår både innkommende og utgående Internett-trafikk og programtilkoblinger, deriblant de som aktivt lytter etter åpne tilkoblinger. Dette gir deg anledning til å se hvilke programmer som kan være åpne for inntrenging, slik at du kan handle deretter.

KAPITTEL 14

Starte Firewall

Så snart du har installert Firewall, er datamaskinen din beskyttet mot inntrenging og uønsket nettverkstrafikk. I tillegg er du klar til å håndtere varsler og administrere innkommende og utgående Internett-tilgang for kjente og ukjente programmer. Smarte anbefalinger og klarering av sikkerhetsnivå (med alternativet satt til tillat programmer kun utgående tilgang til Internett) aktiveres automatisk.

Du kan deaktivere Firewall i ruten Internett- og nettverkskonfigurasjon, men da vil ikke datamaskinen din lenger være beskyttet mot inntrenging og uønsket nettverkstrafikk, og du kan ikke administrere innkommende og utgående Internett-tilkoblinger på en effektiv måte. Hvis du må deaktivere brannmurbeskyttelsen, bør du gjøre det midlertidig og bare når det er nødvendig. Du kan også aktivere Firewall i panelet Internett- og nettverkskonfigurasjon.

Firewall deaktiverer automatisk Windows® Firewall og angir seg selv som standard brannmur.

Merk: Hvis du vil konfigurere Firewall, åpner du ruten Internett- og nettverkskonfigurasjon.

I dette kapitlet

Starte brannmurbeskyttelse 69
Stoppe brannmurbeskyttelse 70

Starte brannmurbeskyttelse

Du kan aktivere Firewall til å beskytte datamaskinen mot inntrenging og uønsket trafikk i tillegg til at du får hjelp til å administrere innkommende og utgående Internett-tilkoblinger.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse deaktivert**, klikker du på **På**.

Stoppe brannmurbeskyttelse

Du kan deaktivere Firewall hvis du ikke ønsker å beskytte datamaskinen fra inntrenging og uønsket trafikk. Hvis Firewall er deaktivert, kan du ikke administrere innkommende eller utgående Internett-tilkoblinger.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Av**.

KAPITTEL 15

Arbeide med varsler

Firewall benytter et bredt spekter av varsler for å hjelpe deg å administrere sikkerheten. Disse varslene kan grupperes i tre grunnleggende typer:

- Rødt varsel
- Gult varsel
- Grønt varsel

Varsler kan også inneholde informasjon som hjelper deg å finne ut hvordan du skal håndtere varsler eller hvordan du kan få informasjon om programmer som kjører på datamaskinen.

I dette kapitlet

Om varsler.....72

Om varsler

Firewall har tre grunnleggende varseltyper. Noen varsler inneholder også informasjon som hjelper deg å lære eller få informasjon om programmer som kjører på datamaskinen din.

Rødt varsel

Et rødt varsel vises når Firewall oppdager og deretter blokkerer en trojansk hest på datamaskinen din og anbefaler at du foretar et søk etter flere trusler. Trojanere ser ut til å være legitime programmer, men kan avbryte, skade eller gi uautorisert tilgang til datamaskinen. Dette varselet forekommer på alle sikkerhetsnivåer, bortsett fra åpent.

Gult varsel

Den vanligste varseltypen er et gult varsel. Det informerer deg om en programaktivitet eller nettverkshendelse oppdaget av Firewall. Når dette forekommer beskriver varselet programaktiviteten eller nettverkshendelsen, og gir deg deretter ett eller flere alternativer som krever en handling fra deg. Varselet **Nytt nettverk oppdaget** vises for eksempel når en datamaskin med Firewall installert kobles til et nytt nettverk. Du kan velge å klarere eller ikke klarere nettverket. Hvis nettverket er klarert, tillater Firewall trafikk fra alle datamaskiner på nettverket og legges til i Klarerte IP-adresser. Hvis Smarte anbefalinger er aktivert, legges programmer til i ruten for programtillatelser.

Grønt varsel

I de fleste tilfeller gir et grønt varsel grunnleggende informasjon om en hendelse uten at det er nødvendig å handle. Grønne varsler deaktiveres som standardinnstilling, og de forekommer vanligvis når sikkerhetsnivåene Standard, Klarert, Høy og Stealth er satt.

Brukerhjelp

Mange Firewall-varsler inneholder tilleggsinformasjon som hjelper deg å administrere datamaskinens sikkerhet, noe som omfatter følgende:

- **Finn ut mer om dette programmet**: Starte McAfees globale webområde om sikkerhet for å få informasjon om et program som Firewall har oppdaget på datamaskinen.
- **Fortell McAfee om dette programmet**: Sende informasjon til McAfee om en ukjent fil som Firewall har oppdaget på datamaskinen.

- **McAfee anbefaler**: Råd om hvordan du håndterer varsler. Et varsel kan for eksempel anbefale at du gir tilgang til et program.

KAPITTEL 16

Håndtere informasjonsvarsler

Med Firewall kan du vise eller skjule informasjonsvarsler når inntrengingsforsøk eller mistenkelige aktiviteter oppdages under bestemte hendelser, for eksempel under fullskjermspilling.

I dette kapitlet

Vise varsler når du spiller.....75
Skjule informasjonsvarsler 75

Vise varsler når du spiller

Med Firewall kan du la informasjonsvarsler vises når inntrengingsforsøk eller mistenkelig aktivitet oppdages under fullskjermspilling.

1. I ruten McAfee SecurityCenter klikker du på **Avansert meny**.
2. Klikk på **Konfigurer**.
3. I ruten SecurityCenter-konfigurasjon klikker du **Varsler** under **Avansert**.
4. I ruten Alternativer for varslinger velger du **Vis informasjonsvarsler når spillmodus er oppdaget**.
5. Klikk **OK**.

Skjule informasjonsvarsler

Du kan forhindre at Firewall-informasjonsvarsler vises når inntrengingsforsøk eller mistenkelig aktivitet oppdages.

1. I ruten McAfee SecurityCenter klikker du på **Avansert meny**.
2. Klikk på **Konfigurer**.
3. I ruten SecurityCenter-konfigurasjon klikker du **Varsler** under **Avansert**.
4. I ruten SecurityCenter-konfigurasjon klikker du på **Informasjonsvarsler**.
5. I ruten Informasjonsvarsler gjør du ett av følgende:
   - Velg **Ikke vis informasjonsvarsler** for å skjule alle informasjonsvarsler.
   - Velg et varsel du vil skjule.
6. Klikk **OK**.

KAPITTEL 17

Konfigurere Firewall-beskyttelse

Firewall tilbyr en rekke metoder for å administrere sikkerheten og skreddersy måten du vil følge opp sikkerhetshendelser og varsler på.

Når du installerer Firewall for første gang, angis beskyttelsesnivået Klarert og programmene tillates kun utgående Internett-tilgang. Firewall tilbyr imidlertid andre nivåer, fra svært restriktiv til svært lite restriktiv.

Firewall gir deg også muligheten til å motta anbefalinger på varsler og Internett-tilgang for programmer.

I dette kapitlet

Administrere sikkerhetsnivåer i Firewall 78
Konfigurere Smarte anbefalinger for varsler 82
Optimalisere Firewall-sikkerhet 84
Sperre og gjenopprette Firewall 87

Administrere sikkerhetsnivåer i Firewall

Firewalls sikkerhetsnivåer kontrollerer i hvilken grad tu vil administrere og reagere på varsler. Disse varslene vises når Firewall oppdager uønsket nettverkstrafikk og innkommende og utgående Internett-tilkoblinger Som standardinnstilling settes Firewalls sikkerhetsnivå til Klarering, med kun utgående tilgang.

Når sikkerhetsnivået Klarering er angitt og Smarte anbefalinger er aktivert, gir gule varsler deg muligheten til å tillate eller blokkere tilgang for ukjente programmer som krever innkommende tilgang. Når kjente programmer oppdages, vises grønne informasjonsvarsler, og det gis automatisk tilgang. Et program som gis tilgang, kan opprette utgående tilkoblinger og lytte etter uanmodede innkommende tilkoblinger.

Generelt sett er det slik at jo mer restriktivt sikkerhetsnivået (Stealth og Høy) er, jo flere alternativer og varsler vises, som du så må håndtere.

Den følgende tabellen beskriver Firewalls seks sikkerhetsnivåer, fra det mest restriktive til det minst restriktive nivået:

Nivå	Beskrivelse
Sperrefunksjonen	Blokkerer alle inngående og utgående nettverkstilkoblinger, inkludert tilgang til webområder, e-post og sikkerhetsoppdateringer. Dette sikkerhetsnivået gir det samme resultatet som å fjerne tilkoblingen til Internett. Du kan bruke denne innstillingen til å blokkere porter du angir som åpen i Systemtjenester-ruten.
Stealth	Blokkerer alle inngående Internett-tilkoblingen, bortsett fra åpne porter, og skjuler datamaskinen din på Internett. Brannmuren varsler deg når nye programmer gjør forsøk på utgående Internett-tilkoblinger eller mottar forespørsler om inngående tilkobling. Blokkerte programmer og programmer som er lagt til, vises i ruten for programtillatelser.
Høy	Varsler deg når nye programmer gjør forsøk på utgående Internett-tilkoblinger eller mottar forespørsler om inngående tilkobling. Blokkerte programmer og programmer som er lagt til, vises i ruten for programtillatelser. Når sikkerhetsnivået angis til Høy, ber et program kun om den typen tilgang som programmet krever på det aktuelle tidspunktet, for eksempel bare utgående tilgang, som du enten kan gi eller blokkere. Hvis programmet senere krever både en innkommende og en utgående tilkobling, kan du gi full tilgang til programmet i ruten for programtillatelser.
Standard	Overvåker innkommende og utgående tilkoblinger og varsler når nye programmer prøver å få Internett-tilgang. Blokkerte programmer og programmer som er lagt til, vises i ruten for programtillatelser.

Klarering	Tillater at programmer har enten inngående og utgående (full) eller kun utgående Internett-tilgang. Standard sikkerhetsnivå er Klarering med alternativet å kun tillate programmer utgående tilgang. Hvis et program tillates full tilgang, vil Firewall automatisk klarere det og legge det til listen over tillatte programmer i ruten Programtillatelser. Hvis et program kun er tillatt utgående tilgang, vil Firewall automatisk klarere det når det kun gjør en utgående Internett-tilkobling. En inngående forbindelse klareres ikke automatisk.
Åpne	Tillater alle innkommende og utgående Internett-tilkoblinger.

Med Firewall kan du også umiddelbart tilbakestille sikkerhetsnivået til Klarering (og tillate kun utgående tilgang) i ruten Gjenopprett standardinnstillinger for Firewall Protection.

Angi sikkerhetsnivået til Sperr

Du kan stille Firewalls sikkerhetsnivå til Sperr for å blokkere alle innkommende og utgående nettverkstilkoblinger

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Sikkerhetsnivå-ruten flytter du glidebryteren slik at **Sperr** vises som gjeldende nivå.
4. Klikk **OK**.

Angi sikkerhetsnivået til Stealth

Du kan stille Firewalls sikkerhetsnivå til Stealth for å blokkere alle inngående nettverkstilkoblinger, bortsett fra åpne porter, for å skjule datamaskinen din på Internett.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Sikkerhetsnivå-ruten flytter du glidebryteren slik at **Stealth** vises som gjeldende nivå.
4. Klikk **OK**.

Merknad: I modusen Stealth vil Firewall varsle deg når nye programmer ber om utgående Internett-tilkobling eller mottar forespørsler om inngående tilkoblinger.

Angi sikkerhetsnivået til Høy

Du Kan stille Firewall-sikkerhetsnivået til Høy, for å motta varslinger om når nye programmer gjør forsøk på utgående Internett-tilkoblinger eller mottar forespørsler om innkommende tilkobling.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Sikkerhetsnivå-ruten flytter du glidebryteren slik at **Høy** vises som gjeldende nivå.
4. Klikk **OK**.

Merknad: I modusen Høy, ber et program kun om den typen tilgang som programmet krever på det aktuelle tidspunktet, for eksempel bare utgående tilgang, som du kan gi eller blokkere. Hvis programmet senere krever både en innkommende og en utgående tilkobling, kan du gi full tilgang til programmet i ruten for programtillatelser.

Angi sikkerhetsnivået til Standard

Du kan angi sikkerhetsnivået til Standard for å overvåke innkommende og utgående tilkoblinger og varsler når nye programmer prøver å få Internett-tilgang.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Sikkerhetsnivå-ruten flytter du glidebryteren slik at **Standard** vises som gjeldende nivå.
4. Klikk **OK**.

Angi sikkerhetsnivået til Klarering

Du kan sette sikkerhetsnivået for Firewall til Klarering for å tillate enten full tilgang eller bare utgående nettverkstilgang.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Sikkerhetsnivå-ruten flytter du glidebryteren slik at **Klarering** vises som gjeldende nivå.
4. Gjør ett av følgende:
   - Velg **Tillat full tilgang** for å tillate full inngående og utgående og nettverkstilgang.

- Velg **Tillat bare utgående tilgang** for å tillate bare utgående nettverkstilgang.

5 Klikk **OK**.

Merknad: Standardinnstilling er **Tillat bare utgående tilgang**.

Angi sikkerhetsnivået til Åpen

Du kan stille Firewalls sikkerhetsnivå til Åpen for å blokkere alle innkommende og utgående nettverkstilkoblinger

1 Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.

2 I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.

3 I Sikkerhetsnivå-ruten flytter du glidebryteren slik at **Åpen** vises som gjeldende nivå.

4 Klikk **OK**.

Konfigurere Smarte anbefalinger for varsler

Du kan konfigurere Firewall slik at varsler inkluderer, utelukker eller viser anbefalinger når programmer prøver å få tilgang til Internett. Ved å aktivere Smarte anbefalinger får du hjelp til å finne ut hvordan du skal håndtere varsler.

Når Smarte anbefalinger er aktivert (og sikkerhetsnivået er satt til Klarere med kun ugående tilgang aktivert), vil Firewall automatisk tillate eller blokkere kjente programmer, og vise en anbefaling i varselet når potensielt farlige programmer oppdages.

Når Smarte anbefalinger er deaktivert, vil Firewall hverken tillate eller blokkere Internett-tilgang og heller ikke anbefale en handlingsplan i varslet.

Når Smarte anbefalinger er satt til Bare Vis, vil et varsel be deg om å tillate eller blokkere tilgang og anbefale en handlingsplan i varselet.

Aktivere Smarte anbefalinger

Du kan aktivere Smarte anbefalinger for Firewall til å automatisk tillate eller blokkere programmer, og varsle deg om ukjente og potensielt farlige programmer.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Sikkerhetsnivå-ruten velger du **Aktiver smarte anbefalinger** under **Smarte anbefalinger**.
4. Klikk **OK**.

Deaktivere Smarte anbefalinger

Du kan deaktivere Smarte anbefalinger for Firewall til å tillate eller blokkere programmer, og varsle deg om ukjente og potensielt farlige programmer. Varslene vil imidlertid utelukke anbefalinger om tilgangshåndtering for programmer. Hvis Firewall oppdager et nytt program som er mistenkelig eller som er kjent for å være en mulig trussel, blokkeres programmet automatisk fra å få tilgang til Internett.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Sikkkerhetsnivå-ruten velger du **Deaktiver smarte anbefalinger** under **Smarte anbefalinger**.
4. Klikk **OK**.

Vise bare Smarte anbefalinger

Du kan vise Smarte anbefalinger for varslene for å motta bare anbefalinger om handlingsplaner slik at du kan avgjøre om du skal tillate eller blokkere ukjente og potensielt farlige programmer.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Sikkerhetsnivå-ruten velger du **Vis bare** under **Smarte anbefalinger**.
4. Klikk **OK**.

Optimalisere Firewall-sikkerhet

Sikkerheten på datamaskinen din kan settes på spill på mange måter. Noen programmer kan for eksempel prøve å koble til Internett før Windows® starter. I tillegg kan sofistikerte datamaskinbrukere spore (eller pinge) datamaskinen for å finne ut om den er koblet til et nettverk. Firewall lar deg forsvare deg mot begge typer inntrenging ved å la deg aktivere beskyttelse under oppstart og blokkere pingforespørsler. Den første innstillingen blokkerer programmer fra å få tilgang til Internett når Windows starter, og den andre blokkerer pingforespørsler som hjelper andre brukere å oppdage datamaskinen din på et nettverk.

Standard installasjonspolicy omfatter automatisk oppdagelse av de vanligste inntrengingsforsøkene, som tjenestenekt (Denial of Service) eller sikkerhetshull. Bruk av standard installasjonspolicy betyr at du beskyttes mot disse angrepene. Du kan imidlertid skru av automatisk oppdagelse for ett eller flere angrep eller søk i ruten for inntrengingsoppdagelse.

Beskytte datamaskinen under oppstart

Du kan beskytte datamaskinen når Windows starter opp ved å blokkere nye programmer som ikke hadde, og nå trenger, Internett-tilgang under oppstart. Firewall viser relevante varsler for programmer som har forespurt om Internett-tilgang. Disse kan du tillate eller blokkere. Når du skal bruke dette alternativet, må ikke sikkerhetsnivået være angitt til Åpen eller Sperr.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Sikkerhetsnivå-ruten velger du **Aktiver beskyttelse under oppstart** under **Sikkerhetsinnstillinger**.
4. Klikk **OK**.

Merk: Blokkerte tilkoblinger og inntrenginger logges ikke når beskyttelse under oppstart er aktivert.

Konfigurere innstillinger for pingforespørsler

Du kan tillate eller forhindre at din datamaskin oppdages på nettverket av andre datamaskiner.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. Under **Sikkerhetsinnstillinger** i Sikkerhetsnivå-ruten gjør du ett av følgende:
   - Velg **Tillat ICMP-pingforespørsler** for å tillate at datamaskinen din oppdages på nettverket ved hjelp av pingforespørsler.
   - Fjern merket for **Tillat ICMP-pingforespørsler** for å hindre at datamaskinen din oppdages på nettverket ved hjelp av pingforespørsler.
4. Klikk **OK**.

Konfigurere inntrengingsoppdagelse

Du kan beskytte datamaskinen fra angrep og uautoriserte søk ved å oppdage inntrengningsforsøk. Standardinnstilling for Firewall inkluderer automatisk oppdagelse av de mest vanlige inntrengningsforsøkene, som Denial of Service-angrep eller sikkerhetshull. Du kan imidlertid deaktivere automatisk oppdagelsen for et eller flere angrep, eller søk.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Inntrengingsoppdagelse**.
4. Under **Oppdag forsøk på inntrenging** gjør du ett av følgende:
   - Velg et navn for å oppdage angrepet eller foreta et søk automatisk.
   - Fjern merket for et navn hvis du vil deaktivere automatisk angrepsoppdagelse eller søk.
5. Klikk **OK**.

Konfigurere beskyttelsesstatusinnstillinger for Firewall

Du kan konfigurere Firewall til å ignorere at spesifikke problemer på datamaskinen ikke rapporteres til SecurityCenter.

1. Klikk **Konfigurer** i ruten McAfee SecurityCenter under **SecurityCenter-informasjon**.
2. I ruten SecurityCenter-konfigurasjon klikker du **Beskyttelsesstatus** under **Avansert**.
3. I ruten Ignorer problemene velger du ett eller flere av følgende alternativer:
   - **Brannmurbeskyttelse er deaktivert.**
   - **Sikkerhetsnivået for brannmuren er satt til Åpen.**
   - **Brannmurtjeneste kjører ikke.**
   - **Firewall-beskyttelse er ikke installert på datamaskinen.**
   - **Windows Firewall er deaktivert.**
   - **Utgående brannmur er ikke installert på datamaskinen.**
4. Klikk **OK**.

Sperre og gjenopprette Firewall

Lockdown blokkerer umiddelbart all inngående og utgående trafikk for å hjelpe deg med å isolere og feilsøke et problem på datamaskinen.

Sperre Firewall øyeblikkelig

Du kan sperre Firewall for å øyeblikkelig blokkere all nettverkstrafikk mellom datamaskinen og Internett.

1. Klikk på **Sperr Firewall** under **Vanlige oppgaver** i ruten McAfee SecurityCenter.
2. I Sperr brannmur-ruten klikker du **Sperr**.
3. Klikk **Ja** for å bekrefte.

Tips: Du kan også sperre Firewall ved å høyreklikke på SecurityCenter-ikonet i systemstatusfeltet til høyre for oppgavelinjen. Klikk deretter på **Hurtiglinker**, og så på **Sperr Firewall**.

Oppheve sperring av brannmuren øyeblikkelig

Du kan sperre Firewall for å øyeblikkelig blokkere all nettverkstrafikk mellom datamaskinen og Internett.

1. Klikk på **Sperr Firewall** under **Vanlige oppgaver** i ruten McAfee SecurityCenter.
2. I ruten Sperrefunksjon aktivert klikker du **Opphev sperring**.
3. Klikk **Ja** for å bekrefte.

Gjenopprette Firewall-innstillinger

Du kan raskt gjenopprette Firewalls opprinnelige beskyttelsesinnstillinger. Dette gjenoppretter sikkerhetsnivået til Klarere og tillater bare utgående nettverkstilgang, aktiverer Smarte anbefalinger, gjenoppretter listen over standardprogrammer og deres tillatelser i ruten Programtillatelser, fjerner klarerte og utestengte IP-adresser, og gjenoppretter systemtjenester, innstillinger for hendelseslogg og inntrengingsoppdagelse.

1. I ruten McAfee SecurityCenter klikker du på **Gjenopprett standardinnstillinger for Firewall**.
2. I ruten Gjenopprett standardinnstillinger for brannmurbeskyttelse klikker du **Gjenopprett standardinnstillingene**.
3. Klikk **Ja** for å bekrefte.

Tips: Du kan også sperre Firewall ved å høyreklikke på SecurityCenter-ikonet i systemstatusfeltet til høyre for oppgavelinjen. Klikk deretter på **Hurtiglinker**, og så på **Sperr Firewall**.

KAPITTEL 18

Administrere programmer og tillatelser

Firewall lar deg administrere og opprette tilgangstillatelser for eksisterende og nye programmer som krever innkommende og utgående Internett-tilgang. Med Firewall kan du kontroller om programmer skal gis full eller bare utgående tilgang. Du kan også blokkere tilgang for programmer.

I dette kapitlet

Tillat Internett-tilgang for programmer 90
Tillat bare utgående tilgang til programmer 92
Blokkere Internett-tilgang for programmer 93
Fjerne tilgangstillatelser for programmer 95
Lære om programmer.....96

Tillat Internett-tilgang for programmer

Enkelte programmer, for eksempel Internett-lesere, trenger tilgang til Internett for å fungere skikkelig.

Firewall lar deg bruke siden for programtillatelser for å:

- Tillat tilgang for programmer
- Tillat bare utgående tilgang til programmer
- Blokkere tilgang for programmer

Du kan også tillate et program full og bare utgående tilgang fra loggene for utgående hendelser og nylige hendelser.

Gi full tilgang til et program

Du kan gi et eksisterende blokkert program på datamaskinen full inngående og utgående tilgang.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Programtillatelser**.
4. Under **Programtillatelser** velger du et program med **Blokkert** eller **Bare utgående tilgang**.
5. Under **Handling** klikker du **Tillat tilgang**.
6. Klikk **OK**.

Gi full tilgang til nytt et program

Du kan gi et nytt program på datamaskinen full inngående og utgående tilgang.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Programtillatelser**.
4. Under **Programtillatelser** klikker du **Legg til tillatt program**.
5. I dialogboksen **Legg til program** blar du etter og velger programmet du vil legge til, og klikker deretter på **Åpne**.

Merk: Du kan endre tillatelsene for et program du har lagt til, på samme måte som for et eksisterende program. Dvs. du velger programmet, og deretter klikker du **Gi bare utgående tilgang** eller **Blokker tilgang** under **Handling**.

Gi full tilgang fra loggen for nylige hendelser

Du kan gi et eksisterende blokkert program som vises i loggen Nylige hendelser full inngående og utgående Internett-tilgang.

1. I ruten McAfee SecurityCenter klikker du på **Avansert meny**.
2. Klikk på**Rapporter og logger**.
3. Under **Nylige hendelser**, velger du hendelsesbeskrivelsen, og deretter klikker du **Tillat tilgang**.
4. I dialogboksen Programtillatelser, klikker du **Ja** for å bekrefte.

Beslektede emner

- Vise utgående hendelser (side 113)

Gi full tilgang fra loggen Utgående hendelser

Du kan gi et eksisterende blokkert program som vises i loggen Utgående hendelser full inngående og utgående Internett-tilgang.

1. I ruten McAfee SecurityCenter klikker du på **Avansert meny**.
2. Klikk på**Rapporter og logger**.
3. I **Nylige hendelser** klikker du på **Vis logg**.
4. Klikk på **Nettverk & Internett**, og klikk deretter på **Utgående hendelser**.
5. Velg et program, og klikk **Tillat tilgang** under **Jeg vil**.
6. I dialogboksen Programtillatelser, klikker du **Ja** for å bekrefte.

Tillat bare utgående tilgang til programmer

Noen programmer på datamaskinen krever utgående Internett-tilgang. Med Firewall kan du konfigurere programtillatelser til å tillate bare utgående Internett-tilgang.

Tillat bare utgående tilgang for et program

Du kan gi et program bare utgående Internett-tilgang.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Programtillatelser**.
4. Under **Programtillatelser** velger du et program med **Blokkert** eller **Full tilgang**.
5. Under **Handling** klikker du **Tillat bare utgående tilgang**.
6. Klikk **OK**.

Tillat bare utgående tilgang fra loggen Nylige hendelser

Du kan gi et eksisterende blokkert program som vises i loggen Nylige hendelser bare utgående Internett-tilgang.

1. I ruten McAfee SecurityCenter klikker du på **Avansert meny**.
2. Klikk på**Rapporter og logger**.
3. Under **Nylige hendelser**, velger du hendelsesbeskrivelsen, og deretter klikker du **Tillat bare utgående tilgang**.
4. I dialogboksen Programtillatelser, klikker du **Ja** for å bekrefte.

Tillat bare utgående tilgang fra loggen for utgående hendelser

Du kan gi et eksisterende blokkert program som vises i loggen Utgående hendelser bare utgående Internett-tilgang.

1. I ruten McAfee SecurityCenter klikker du på **Avansert meny**.
2. Klikk på**Rapporter og logger**.
3. I **Nylige hendelser** klikker du på **Vis logg**.
4. Klikk på **Nettverk & Internett**, og klikk deretter på **Utgående hendelser**.
5. Velg et program, og klikk **Tillat bare utgående tilgang** under **Jeg vil**.
6. I dialogboksen Programtillatelser, klikker du **Ja** for å bekrefte.

Blokkere Internett-tilgang for programmer

Med Firewall kan du blokkere programmer fra å få tilgang til Internett. Kontroller at ikke nettverkstilkoblingen avbrytes eller at et annet program som krever tilgang til Internett for å fungere skikkelig, forstyrres når du blokkerer et program.

Blokkere tilgang for et program

Du kan blokkere et program fra å ha inngående og utgående Internett-tilgang.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Programtillatelser**.
4. Under **Programtillatelser** velger du et program med **Full tilgang** eller **Bare utgående tilgang**.
5. Under **Handling** klikker du **Blokker tilgang**.
6. Klikk **OK**.

Blokkere tilgangen for et nytt program

Du kan blokkere et nytt program fra å ha inngående og utgående Internett-tilgang.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Programtillatelser**.
4. Under **Programtillatelser** klikker du **Legg til blokkert program**.
5. I dialogboksen Legg til program, blar du etter og velger programmet du vil legge til, og klikker deretter på **Åpne**.

Merk: Du kan endre tillatelsene for et program du har lagt til ved å velge programmet, og deretter klikke på **Tillat bare utgående tilgang** eller **Tillat tilgang** under **Handling**.

Blokkere tilgang fra loggen for nylige hendelser

Du kan blokkere et program som vises i loggen Nylige hendelser slik at det ikke vil ha inngående og utgående Internett-tilgang.

1. I ruten McAfee SecurityCenter klikker du på **Avansert meny**.
2. Klikk på**Rapporter og logger**.
3. Under **Nylige hendelser**, velger du hendelsesbeskrivelsen, og deretter klikker du **Blokker tilgang**.
4. I dialogboksen Programtillatelser, klikker du **Ja** for å bekrefte.

Fjerne tilgangstillatelser for programmer

Før du fjerner en programtillatelse, må du forsikre deg om at fraværet av dette programmet ikke påvirker datamaskinens funksjonalitet eller nettverkstilkoblingen din.

Fjerne en programtillatelse

Du kan fjerne et program fra å ha inngående eller utgående Internett-tilgang.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Programtillatelser**.
4. Under **Programtillatelser** velger du et program.
5. Under **Handling** klikker du **Fjern programtillatelse**.
6. Klikk **OK**.

Merk: Firewall hindrer deg i å endre enkelte programmer ved å tone ned og deaktivere visse handlinger.

Lære om programmer

Hvis du er usikker på hvilken programtillatelse du skal bruke, kan du få informasjon om programmet på McAfees webområde HackerWatch.

Få programinformasjon

Du kan få programinformasjon for å avgjøre om du skal tillate eller blokkere inngående og utgående Internett-tilgang på McAfees webområde HackerWatch.

Merknad: Pass på at du er koblet til Internett slik at webleseren kan starte McAfees HackerWatch-webområde, som gir oppdatert informasjon og programmer, Internett-tilgangskrav og sikkerhetstrusler.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Programtillatelser**.
4. Under **Programtillatelser** velger du et program.
5. Under **Handling** klikker du **Mer informasjon**.

Få programinformasjon fra loggen for utgående hendelser

Du kan få programinformasjon fra loggen Utgående hendelser for å avgjøre for hvilke programmer du skal tillate eller blokkere inngående og utgående Internett-tilgang på McAfees webområde HackerWatch.

Merknad: Pass på at du er koblet til Internett slik at webleseren kan starte McAfees HackerWatch-webområde, som gir oppdatert informasjon og programmer, Internett-tilgangskrav og sikkerhetstrusler.

1. I ruten McAfee SecurityCenter klikker du på **Avansert meny**.
2. Klikk på**Rapporter og logger**.
3. Velg en hendelse under Nylige hendelser og klikk deretter på **Vis logg**.
4. Klikk på **Nettverk & Internett**, og klikk deretter på **Utgående hendelser**.
5. Velg en IP-adresse, og klikk deretter **Lær mer**.

KAPITTEL 19

Behandle systemtjenester

For at enkelte programmer (for eksempel webtjenere og tjenerprogrammer for fildeling) skal fungere riktig, må de godta uanmodede tilkoblinger fra andre datamaskiner via angitte systemtjenesteporter. Vanligvis lukker Firewall disse systemtjenesteportene fordi de utgjør den største kilden til sikkerhetshull og sårbarheter i systemet. For å godta tilkoblinger fra eksterne datamaskiner må imidlertid systemtjenesteportene være åpne.

I dette kapitlet

Konfigurere systemtjenesteporter 98

Konfigurere systemtjenesteporter

Systemtjenesteporter kan konfigureres til å tillate eller blokkere ekstern nettverkstilgang til en tjeneste på din datamaskin.

Listen nedenfor viser de vanlige systemtjenestene og dere tilknyttede porter.

- Filoverføringsprotokollporter (FTP) 20-21
- E-posttjenerport (IMAP) 143
- E-posttjenerport (POP3) 110
- E-posttjenerport (SMTP) 25
- Microsofts katalogtjenerport (MSFT DS) 445
- Microsoft SQL Server-port (MSFT SQL) 1433
- Network Time Protocol Port 123
- Port 3389 for Remote Desktop / Remote Assistance / Terminal Server (RDP)
- RPC-kallport (Remote Procedure Calls) 135
- Sikker webtjenerport (HTTPS) 443
- Universal Plug and Play-port (UPNP) 5000
- Webtjenerport (HTTP) 80
- Fildelingsporter i Windows (NETBIOS) 137-139

Systemtjenesteporter kan også konfigureres til å tillate at en datamaskin deler Internett-tilkoblingene med andre datamaskiner koblet til den gjennom det samme nettverket. Denne forbindelsen, kjent som ICS (Internet Connection Sharing), tillater at datamaskinen deler forbindelsen for å fungere som en gateway to Internett for de andre datamaskinene i nettverket.

Merknad: Hvis datamaskinen din har et program som tillater enten Internett- eller FTP-servertilkoblinger, må datamaskinen som deler tilkoblingen åpne den tilknyttede systemtjenesteporten og tillate videresending av innkommende tilkoblinger for disse portene.

Tillat tilgang til en eksisterende systemtjenesteport

Du kan åpne en eksisterende port for å tillate ekstern tilgang til en nettverkstjeneste på din datamaskin.

Merknad: En åpen systemtjenesteport kan gjøre datamaskinen sårbar for Internett-sikkerhetstrusler. Åpne derfor bare en port hvis det er nødvendig.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Systemtjenester**.
4. Under **Åpne systemtjenesteport** velger du en systemtjeneste for å åpne porten for tjenesten.
5. Klikk **OK**.

Blokkere tilgang til en eksisterende systemtjenesteport

Du kan lukke en eksisterende port for å blokkere ekstern nettverkstilgang til en tjeneste på din datamaskin.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Systemtjenester**.
4. Under **Åpne systemtjenesteport** fjerner du merket for en systemtjeneste for å lukke tjenestens port.
5. Klikk **OK**.

Konfigurere en ny systemtjenesteport

Du kan konfigurere en ny nettverkstjenesteport på datamaskinen som du kan åpne eller lukke for å tillate eller blokkere ekstern tilgang på datamaskinen.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Systemtjenester**.
4. Klikk på **Legg til**.
5. I ruten System Services, under **Porter og systemtjenester**, legger du inn følgende:
   - Programnavn
   - Innkommende TCP/IP-porter

- Utgående TCP/IP-porter
- Innkommende UDP-porter
- Utgående UDP-porter

6 Hvis du vil sende aktivitetsinformasjonen for denne porten til en annen datamaskin i Windwos-nettverket som deler din Internett-tilkobling, velger du **Videresend nettverksaktivitet på denne porten til nettverksbrukere som bruker Deling av Internett-tilkobling**.

7 Beskriv eventuelt den nye konfigurasjonen.

8 Klikk **OK**.

Merknad: Hvis datamaskinen din har et program som tillater enten Internett- eller FTP-servertilkoblinger, må datamaskinen som deler tilkoblingen åpne den tilknyttede systemtjenesteporten og tillate videresending av innkommende tilkoblinger for disse portene. Hvis du bruker deling av Internett-tilkobling (ICS) må du også legge til en klarert dataforbindelse på listen over klarerte IP-adresser. Se Legg til en klarert datamaskintilkobling for mer informasjon.

Endre en systemtjenesteport

Du kan endre informasjonen om inngående og utgående nettverkstilgang for en eksisterende systemtjenesteport.

Merknad: Hvis portinformasjonen angis på feil måte, mislykkes systemtjenesten.

1 Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.

2 I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.

3 I Brannmur-ruten klikker du **Systemtjenester**.

4 Velg en systemtjeneste, og klikk **Rediger**.

5 I ruten System Services, under **Porter og systemtjenester**, legger du inn følgende:

- Programnavn
- Innkommende TCP/IP-porter
- Utgående TCP/IP-porter
- Innkommende UDP-porter
- Utgående UDP-porter

6 Hvis du vil sende aktivitetsinformasjonen for denne porten til en annen datamaskin i Windwos-nettverket som deler din Internett-tilkobling, velger du **Videresend nettverksaktivitet på denne porten til nettverksbrukere som bruker Deling av Internett-tilkobling**.

7 Beskriv eventuelt den endrede konfigurasjonen.

8 Klikk **OK**.

Fjerne en systemtjenesteport

Du kan fjerne en eksisterende systemtjenesteport fra datamaskinen. Etter at porten er fjernet, har ikke lenger eksterne datamaskiner tilgang til nettverkstjenesten på din datamaskin.

1 Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.

2 I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.

3 I Brannmur-ruten klikker du **Systemtjenester**.

4 Velg en systemtjeneste, og klikk deretter **Fjern**.

5 Når du blir spurt, klikk **Ja** for å bekrefte.

KAPITTEL 20

Administrere datamaskintilkoblinger

Du kan konfigurere Firewall til å administrere bestemte eksterne tilkoblinger til datamaskinen ved å opprette regler basert på Internett-protokolladresser (IP-adresser) som er tilknyttet eksterne datamaskiner. Datamaskiner som er tilknyttet klarerte IP-adresser, kan trygt tilkobles datamaskinen din, mens datamaskiner som er tilknyttet IP-adresser som er ukjente, mistenkelige eller mistrodde, kan bli utestengt fra å kobles til datamaskinen din.

Når du tillater en tilkobling, må du passe på at datamaskinen du klarerer, er sikker. Hvis en datamaskin som du har klarert, er infisert med en orm eller en annen mekanisme, kan datamaskinen din være sårbar for infeksjon. McAfee anbefaler også at datamaskinen(e) du klarerer, er beskyttet av en brannmur og et oppdatert antivirusprogram. Firewall logger ikke trafikk og genererer heller ikke hendelsesvarsler fra IP-adresser i listen over klarerte IP-adresser.

Datamaskiner forbundet med ukjente, mistenkelige eller mistrodde IP-adresser kan få forbud mot å kobles til datamaskinen din.

Ettersom Firewall blokkerer all uønsket trafikk, er det vanligvis ikke nødvendig å utestenge IP-adresser. Du bør bare utestenge en IP-adresse når du er sikker på at en Internett-tilkobling utgjør en bestemt trussel. Sørg for at du ikke blokkerer viktige IP-adresser, for eksempel DNS- eller DHCP-tjeneren eller andre ISP-tjenere. Firewall kan gi melding når den oppdager en handling fra en utestengt datamaskin, alt etter hvilke sikkerhetsinnstillinger du har.

I dette kapitlet

Klarere datamaskintilkoblinger.....104
Stenge ute datamaskintilkoblinger 107

Klarere datamaskintilkoblinger

Du kan legge til, redigere og fjerne klarerte IP-adresser i ruten Klarerte og utestengte IP-adresser under **Klarerte IP-adresser**.

Ved hjelp av listen **Klarerte IP-adresser** i ruten for klarerte og utestengte IP-adresser kan du bestemme at all trafikk fra en bestemt datamaskin skal leveres til datamaskinen din. Firewall logger ikke trafikk og genererer heller ikke hendelsesvarsler fra IP-adresser som vises i listen **Klarerte IP-adresser**.

Firewall stoler på alle avmerkede IP-adresser på listen og tillater alltid trafikk fra en klarert IP gjennom brannmuren på hvilken som helst port. Aktivitet mellom datamaskinen som er tilknyttet en klarert IP-adresse, og din datamaskin filtreres eller analyseres ikke av Firewall. Som standardinnstiling er listene over klarerte IP-adresser det første nettverket som Firewall finner.

Når du tillater en tilkobling, må du passe på at datamaskinen du klarerer, er sikker. Hvis en datamaskin som du har klarert, er infisert med en orm eller en annen mekanisme, kan datamaskinen din være sårbar for infeksjon. McAfee anbefaler også at datamaskinen(e) du klarerer, er beskyttet av en brannmur og et oppdatert antivirusprogram.

Legge til en klarert datamaskintilkobling

Du kan legge til en klarert datamaskintilkobling og tilkoblingens tilknyttede IP-adresse.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Klarerte og utestengte IP-adresser**.
4. I ruten Klarerte og utestengte IP-adresser velger du **Klarerte IP-adresser**, og deretter klikker du **Legg til**.
5. Under **Legg til regel om klarert IP-adresse** gjør du ett av følgende:
   - Velg **Enkel IP-adresse**, og angi deretter IP-adressen.
   - Velg **IP-adresseområde**, og angi deretter start- og sluttadresser i boksene **Fra IP-adresse** og **Til IP-adresse**.

6 Hvis en systemtjeneste bruke deling av Internett-tilkobling (ICS) kan du legge til følgende IP-adresseområde: 192.168.0.1 til 192.168.0.255.

7 Velg eventuelt **Regel utløper om**, og angi hvor mange dager regelen skal gjelde.

8 Skriv eventuelt inn en beskrivelse av regelen.

9 Klikk **OK**.

10 Klikk **Ja** for å bekrefte i dialogboksen **Klarerte og utestengte IP-adresser**.

Merknad: For mer informasjon om deling av Internett-tilkobling (ICS) kan du se Konfigurere en ny systemtjeneste.

Legge til en klarert datamaskin fra loggen for innkommende hendelser

Du kan legge til en klarert datamaskintilkobling og koblingens tilknyttede IP-adresse fra loggen for innkommende hendelser.

1 Klikk på **Avansert meny** under Vanlige oppgaver i Ruten McAfee SecurityCenter.

2 Klikk på**Rapporter og logger**.

3 I **Nylige hendelser** klikker du på **Vis logg**.

4 Klikk på **Nettverk & Internett** og deretter på **Innkommende hendelser**.

5 Velg en kilde-IP-adresse, og klikk **Klarer denne adressen** under **Jeg vil**.

6 Klikk **Ja** for å bekrefte.

Redigere en klarert datamaskintilkobling

Du kan redigere en klarert datamaskintilkobling og tilkoblingens tilknyttede IP-adresse.

1 Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.

2 I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.

3 I Brannmur-ruten klikker du **Klarerte og utestengte IP-adresser**.

4 I ruten Klarerte og utestengte IP-adresser velger du **Klarerte IP-adresser**.

5 Velg en IP-adresse, og klikk deretter **Rediger**.

6 Under **Rediger klarert IP-adresse** gjør du ett av følgende:

- Velg **Enkel IP-adresse**, og angi deretter IP-adressen.

- Velg **IP-adresseområde**, og angi deretter start- og sluttadresser i boksene **Fra IP-adresse** og **Til IP-adresse**.

7 Merk eventuelt av for **Regel utløper om**, og angi hvor mange dager regelen skal gjelde.

8 Skriv eventuelt inn en beskrivelse av regelen.

9 Klikk **OK**.

Merknad: Du kan ikke redigere standard datamaskintilkobling(er) som Firewall automatisk har lagt til fra et klarert privat nettverk.

Fjerne en klarert datamaskintilkobling

Du kan fjerne en klarert datamaskintilkobling og tilkoblingens tilknyttede IP-adresse.

1 Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.

2 I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.

3 I Brannmur-ruten klikker du **Klarerte og utestengte IP-adresser**.

4 I ruten Klarerte og utestengte IP-adresser velger du **Klarerte IP-adresser**.

5 Velg en IP-adresse, og klikk deretter **Fjern**.

6 Klikk **Ja** for å bekrefte i dialogboksen **Klarerte og utestengte IP-adresser**.

Stenge ute datamaskintilkoblinger

Du kan legge til, redigere og fjerne utestengte IP-adresser i Klarerte og utestengte IP-adresser under **Utestengte IP-adresser**.

Datamaskiner forbundet med ukjente, mistenkelige eller mistrodde IP-adresser kan få forbud mot å kobles til datamaskinen din.

Ettersom Firewall blokkerer all uønsket trafikk, er det vanligvis ikke nødvendig å utestenge IP-adresser. Du bør bare utestenge en IP-adresse når du er sikker på at en Internett-tilkobling utgjør en bestemt trussel. Sørg for at du ikke blokkerer viktige IP-adresser, for eksempel DNS- eller DHCP-tjeneren eller andre ISP-tjenere. Firewall kan gi melding når den oppdager en handling fra en utestengt datamaskin, alt etter hvilke sikkerhetsinnstillinger du har.

Legge til en utestengt datamaskintilkobling

Du kan legge til en utestengt datamaskintilkobling og tilkoblingens tilknyttede IP-adresse.

Merknad: Sørg for at du ikke blokkerer viktige IP-adresser, for eksempel DNS- eller DHCP-tjeneren eller andre ISP-tjenere.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Klarerte og utestengte IP-adresser**.
4. I ruten Klarerte og utestengte IP-adresser velger du **Utestengte IP-adresser**, og deretter klikker du **Legg til**.
5. Under **Legg til regel om utestengt IP-adresse**, gjør du ett av følgende:
   - Velg **Enkel IP-adresse**, og angi deretter IP-adressen.
   - Velg **IP-adresseområde**, og angi deretter start- og sluttadresser i boksene **Fra IP-adresse** og **Til IP-adresse**.
6. Velg eventuelt **Regel utløper om**, og angi hvor mange dager regelen skal gjelde.
7. Skriv eventuelt inn en beskrivelse av regelen.
8. Klikk **OK**.
9. Klikk **Ja** for å bekrefte i dialogboksen **Klarerte og utestengte IP-adresser**.

Redigere en utestengt datamaskintilkobling

Du kan redigere en utestengt datamaskintilkobling og tilkoblingens tilknyttede IP-adresse.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Klarerte og utestengte IP-adresser**.
4. I ruten Klarerte og utestengte IP-adresser velger du **Utestengte IP-adresser**, og deretter klikker du **Rediger**.
5. Under **Rediger utestengt IP-adresse** gjør du ett av følgende:
   - Velg **Enkel IP-adresse**, og angi deretter IP-adressen.
   - Velg **IP-adresseområde**, og angi deretter start- og sluttadresser i boksene **Fra IP-adresse** og **Til IP-adresse**.
6. Velg eventuelt **Regel utløper om**, og angi hvor mange dager regelen skal gjelde.
7. Skriv eventuelt inn en beskrivelse av regelen.
8. Klikk **OK**.

Fjerne en utestengt datamaskintilkobling

Du kan fjerne en utestengt datamaskintilkobling og tilkoblingens tilknyttede IP-adresse.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Klarerte og utestengte IP-adresser**.
4. I ruten Klarerte og utestengte IP-adresser velger du **Utestengte IP-adresser**.
5. Velg en IP-adresse, og klikk deretter **Fjern**.
6. Klikk **Ja** for å bekrefte i dialogboksen **Klarerte og utestengte IP-adresser**.

Stenge ute en datamaskin fra loggen for innkommende hendelser

Du kan stenge ute en datamaskintilkobling og tilkoblingens tilknyttede IP-adresse fra loggen for innkommende hendelser.

IP-adressene som vises i loggen for innkommende hendelser, blokkeres. Du oppnår derfor ingen ekstra beskyttelse ved å stenge ute en adresse, med mindre datamaskinen enten bruker porter som eksplisitt er åpnet, eller med mindre datamaskinen din har et program som har fått Internett-tilgang.

Du bør bare legge til en IP-adresse i listen **Utestengte IP-adresser** hvis du har åpnet én eller flere porter, og hvis du har grunn til å tro at du må blokkere adressens tilgang til åpne porter.

Du kan bruke siden for innkommende hendelser, som viser IP-adressene til all innkommende Internett-trafikk, til å stenge ute en IP-adresse du tror er kilden til mistenkelig eller uønsket Internett-aktivitet.

1. Klikk på **Avansert meny** under **Vanlige oppgaver** i ruten McAfee SecurityCenter.
2. Klikk på**Rapporter og logger**.
3. I **Nylige hendelser** klikker du på **Vis logg**.
4. Klikk på **Nettverk & Internett** og deretter på **Innkommende hendelser**.
5. Velg en kilde-IP-adresse, og klikk **Utesteng denne adressen** under **Jeg vil**.
6. Klikk **Ja** for å bekrefte i dialogboksen **Legg til regel om utestengt IP-adresse**.

Stenge ute en datamaskin fra loggen for inntrengingsoppdagelseshendelser

Du kan stenge ute en datamaskintilkobling og tilkoblingens tilknyttede IP-adresse fra loggen for inntrengingsoppdagelseshendelser.

1. Klikk på **Avansert meny** under **Vanlige oppgaver** i ruten McAfee SecurityCenter.
2. Klikk på**Rapporter og logger**.
3. I **Nylige hendelser** klikker du på **Vis logg**.
4. Klikk **Nettverk & og Internett**, og klikk deretter **Inntrengingsoppdagelseshendelser**.
5. Velg en kilde-IP-adresse, og klikk **Utesteng denne adressen** under **Jeg vil**.
6. Klikk **Ja** for å bekrefte i dialogboksen **Legg til regel om utestengt IP-adresse**.

KAPITTEL 21

Logge, overvåke og analysere

Firewall tilbyr omfattende og lettlest logging, overvåking og analyse for Internett-hendelser og -trafikk. Å forstå Internett-trafikk og -hendelser kan være til hjelp når du skal administrere Internett-tilkoblingene dine.

I dette kapitlet

Hendelseslogging 112
Arbeide med statistikk 114
Spore Internett-trafikk 115
Overvåke Internett-trafikk 118

Hendelseslogging

Firewall lar deg aktivere eller deaktivere logging og hvilke hendelsestyper som skal logges når logging er aktivert. Hendelseslogging lar deg vise de siste innkommende og utgående hendelsene samt inntrengningshendelser.

Konfigurere innstillinger for hendelseslogg

Du kan angi og konfigurere alle typer Firewall-hendelser for logging. Som standardinnstilling er hendelseslogg aktivert for alle hendelser og aktiviteter.

1. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
2. I Brannmur-ruten klikker du **Innstillinger for hendelseslogg**.
3. Velg **Aktiver hendelseslogging** hvis det ikke allerede er valgt.
4. Under **Aktiver hendelseslogging** velger eller sletter du hendelsestyper som du ønsker eller ikke ønsker å logge. Hendelsestypene omfatter følgende:
   - Blokkerte programmer
   - ICMP-pinger
   - Trafikk fra utestengte IP-adresser
   - Hendelser på systemtjenesteporter
   - Hendelser på ukjente porter
   - Inntrengingsoppdagelseshendelser (IDS)
5. Hvis du vil hindre logging på bestemte porter, velger du **Ikke logg hendelser på følgende port(er)**, og deretter angir du enkelte portnumre atskilt med kommaer, eller portområder med bindestreker. For eksempel `137-139, 445, 400-5000`.
6. Klikk **OK**.

Vise nylige hendelser

Hvis logging er aktivert, kan du vise de nyeste hendelsene. Ruten Nylige hendelser viser datoen for og en beskrivelse av hendelsen. Det viser aktivitet for programmer som tilgang til Internett er blokkert for.

- Under Vanlige oppgaver på **Avansert meny** klikker du **Rapporter og logger** eller **Vis nyeste hendelser**. Du kan eventuelt klikke **Vis nyeste hendelser** under ruten Vanlige oppgaver fra Grunnleggende meny.

Vise innkommende hendelser

Hvis logging er aktivert, kan du vise innkommende hendelser. Innkommende hendelser inkluderer dato og tidspunkt, kildt-IP-adresse, vertsnavn og informasjon og hendelsestype.

1. Pass på at den avanserte menyen er aktivert. I Vanlige oppgaver-ruten klikker du på **Rapporter og logger**.
2. I **Nylige hendelser** klikker du på **Vis logg**.
3. Klikk på **Nettverk & Internett** og deretter på **Innkommende hendelser**.

Merk: Du kan klarere, stenge ute og spore en IP-adresse fra loggen for innkommende hendelser.

Vise utgående hendelser

Hvis logging er aktivert, kan du vise utgående hendelser. Utgående hendelser omfatter navnet på programmet som prøver å få utgående tilgang, dato og klokkeslett for hendelsen og programmets plassering på datamaskinen.

1. I Vanlige oppgaver-ruten klikker du på **Rapporter og logger**.
2. I **Nylige hendelser** klikker du på **Vis logg**.
3. Klikk på **Nettverk & Internett**, og klikk deretter på **Utgående hendelser**.

Merk: Du kan gi full tilgang og bare utgående tilgang til et program fra loggen for utgående hendelser. Du kan også finne tilleggsinformasjon om programmet.

Vise inntrengingsoppdagelseshendelser

Hvis logging er aktivert, kan du vise innkommende inntrengingshendelser. Inntrengingsoppdagelseshendelser viser dato og klokkeslett, kilde-IP, vertsnavnet for hendelsen og hendelsestypen.

1. I Vanlige oppgaver-ruten klikker du på **Rapporter og logger**.
2. I **Nylige hendelser** klikker du på **Vis logg**.
3. Klikk **Nettverk & og Internett**, og klikk deretter **Inntrengingsoppdagelseshendelser**.

Merk: Du kan stenge ute og spore en IP-adresse fra loggen for inntrengingsoppdagelseshendelser.

Arbeide med statistikk

Firewall benytter McAfees HackerWatch-webområde om sikkerhet for å gi deg statistikk om globale Internett-sikkerhetshendelser og -portaktivitet.

Vise statistikk for globale sikkerhetshendelser

HackerWatch sporer globale Internett-sikkerhetshendelser som du kan vise fra SecurityCenter. Sporet informasjon omfatter hendelser som er rapportert til HackerWatch de siste 24 timene, 7 dagene og 30 dagene.

1. Kontroller at Avansert meny er aktivert, og klikk deretter **Verktøy**.
2. I Verktøy-ruten klikker du **HackerWatch**.
3. Vis statistikk for sikkerhetshendelser under Event Tracking.

Vise global Internett-portaktivitet

HackerWatch sporer globale Internett-sikkerhetshendelser som du kan vise fra SecurityCenter. Informasjonen som vises, inkluderer portene med høyest hendelsesforekomst rapportert til HackerWatch de siste sju dagene. Vanligvis vises HTTP-, TCP- og UDP-informasjon.

1. Kontroller at Avansert meny er aktivert, og klikk deretter **Verktøy**.
2. I Verktøy-ruten klikker du **HackerWatch**.
3. Vis portene med høyest hendelsesforekomst under **Recent Port Activity** (Nyeste portaktivitet).

Spore Internett-trafikk

Firewall tilbyr en rekke alternativer for å spore Internett-trafikk. Disse alternativene lar deg spore en nettverksdatamaskin geografisk, få domene- og nettverksinformasjon samt spore datamaskiner fra loggene for innkommende hendelser og inntrengingsoppdagelseshendelser.

Spore en nettverksdatamaskin geografisk

Du kan bruke Visuell sporing til å finne ut hvor en datamaskin som kobler seg til eller prøver å koble seg til datamaskinen din, befinner seg geografisk, ved hjelp av navnet eller IP-adressen. Du kan også få tilgang til nettverks- og registreringsinformasjon ved hjelp av Visuell sporing. Når du kjører Visuell sporing, vises et verdenskart som viser den mest sannsynlige ruten data har tatt fra kildedatamaskinen til din maskin.

1. Kontroller at Avansert meny er aktivert, og klikk deretter **Verktøy**.
2. I Verktøy-ruten klikker du **Visuell sporing**.
3. Skriv inn datamaskinens IP-adresse, og klikk **Spor**.
4. Under **Visuell sporing** velger du **Kartvisning**.

Merk: Du kan ikke spore private eller ugyldige IP-hendelser eller hendelser som går i løkke.

Få registreringsinformasjonen til en datamaskin

Du kan få registreringsinformasjonen til en datamaskin fra SecurityCenter ved hjelp av Visuell sporing. Informasjon inneholder domenenavnet, registrertes navn og adresse og administrasjonskontakt.

1. Kontroller at Avansert meny er aktivert, og klikk deretter **Verktøy**.
2. I Verktøy-ruten klikker du **Visuell sporing**.
3. Skriv inn datamaskinens IP-adresse, og klikk deretter **Spor**.
4. Under **Visuell sporing** velger du **Registreringsvisning**.

Få nettverksinformasjonen til en datamaskin

Du kan få nettverksinformasjonen til en datamaskin fra SecurityCenter ved hjelp av Visuell sporing. Nettverksinformasjon inneholder detaljer om nettverket der domenet ligger.

1. Kontroller at Avansert meny er aktivert, og klikk deretter **Verktøy**.
2. I Verktøy-ruten klikker du **Visuell sporing**.
3. Skriv inn datamaskinens IP-adresse, og klikk deretter **Spor**.
4. Under **Visuell sporing** velger du **Nettverksvisning**.

Spore en datamaskin fra loggen for innkommende hendelser

I ruten for innkommende hendelser kan du spore en IP-adresse som vises i loggen for innkommende hendelser.

1. Pass på at den avanserte menyen er aktivert. I Vanlige oppgaver-ruten klikker du på **Rapporter og logger**.
2. I **Nylige hendelser** klikker du på **Vis logg**.
3. Klikk på **Nettverk & Internett** og deretter på **Innkommende hendelser**.
4. I ruten for innkommende hendelser velger du en kilde-IP-adresse, og deretter klikker du **Spor denne adressen**.
5. I ruten Visuell sporing klikker du én av følgende:
   - **Kartvisning**: Finne en datamaskin geografisk ved hjelp av den valgte IP-adressen.
   - **Registreringsvisning**: Finne domeneinformasjon ved hjelp av den valgte IP-adressen.
   - **Nettverksvisning**: Finne nettverksinformasjon ved hjelp av den valgte IP-adressen.
6. Klikk på **Fullført**.

Spore en datamaskin fra loggen for inntrengingsoppdagelseshendelser

I ruten for inntrengingsoppdagelseshendelser kan du spore en IP-adresse som vises i loggen for inntrengingsoppdagelseshendelser.

1. I Vanlige oppgaver-ruten klikker du på **Rapporter og logger**.
2. I **Nylige hendelser** klikker du på **Vis logg**.
3. Klikk **Nettverk & og Internett**, og klikk deretter **Inntrengingsoppdagelseshendelser**. I ruten for inntrengingsoppdagelseshendelser velger du en kilde-IP-adresse, og deretter klikker du **Spor denne adressen**.
4. I ruten Visuell sporing klikker du én av følgende:
   - **Kartvisning**: Finne en datamaskin geografisk ved hjelp av den valgte IP-adressen.

- **Registreringsvisning**: Finne domeneinformasjon ved hjelp av den valgte IP-adressen.
- **Nettverksvisning**: Finne nettverksinformasjon ved hjelp av den valgte IP-adressen.

5 Klikk på **Fullført**.

Spore en overvåket IP-adresse

Du kan spore en overvåket IP-adresse for å få en geografisk visning som viser den mest sannsynlige ruten for data fra kildedatamaskinen til din egen. I tillegg kan du få registrerings- og nettverksinformasjon om IP-adressen.

1 Kontroller at Avansert meny er aktivert, og klikk **Verktøy**.

2 I Verktøy-ruten klikker du **Trafikkovervåking**.

3 Under **Trafikkovervåking** klikker du **Aktive programmer**.

4 Velg et program og deretter IP-adressen som vises under programnavnet.

5 Under **Programaktivitet** klikker du **Spor denne IP-adressen**.

6 Under **Visuell sporing** kan du vise et kart som viser den mest sannsynlige ruten for data fra kildedatamaskinen til din egen. I tillegg kan du få registrerings- og nettverksinformasjon om IP-adressen.

Merk: Hvis du vil vise den mest oppdaterte statistikken, klikker du **Oppdater** under **Visuell sporing**.

Overvåke Internett-trafikk

Firewall inneholder en rekke metoder for å overvåke Internett-trafikken, inkludert følgende:

- **Diagrammet Trafikkanalyse**: Viser nylig innkommende og utgående Internett-trafikk.
- **Diagrammet Trafikkbruk**: Viser prosentandelen av båndbredden brukt av de mest aktive programmene den siste 24-timersperioden.
- **Aktive programmer**: Viser de programmene som for øyeblikket bruker flest nettverkstilkoblinger på datamaskinen, og IP-adressene som programmene har tilgang til.

Om diagrammet Trafikkanalyse

Trafikkanalysediagrammet er en numerisk og grafisk representasjon av innkommende og utgående Internett-trafikk. Trafikkovervåking viser også hvilke programmer som bruker de fleste nettverkstilkoblingene på datamaskinen, og hvilke IP-adresser applikasjonene åpner.

I Trafikkanalyse-ruten kan du vise den siste innkommende og utgående Internett-trafikken samt gjeldende, gjennomsnittlige og maksimale overføringshastigheter. Du kan også vise trafikkvolum, inkludert trafikkmengden siden du startet Firewall, og den totale trafikken for gjeldende måned og tidligere måneder.

Trafikkanalyse-ruten viser Internett-aktivitet på datamaskinen i sanntid, inkludert volumet og hastigheten på den nylig innkommende og utgående Internett-trafikken på datamaskinen, tilkoblingshastighet og totalt antall byte som er overført over Internett.

Den heltrukne grønne streken representerer gjeldende overhøringshastighet for innkommende trafikk. Den prikkete grønne streken representerer gjennomsnittlig overføringshastighet for innkommende trafikk. Hvis gjeldende overføringshastighet og gjennomsnittlig overføringshastighet er den samme, vises ikke den prikkete streken på diagrammet. Den heltrukne streken representerer både gjennomsnittlig og gjeldende overføringshastighet.

Den heltrukne røde streken representerer gjeldende overføringshastighet for utgående trafikk. Den røde prikkete streken representerer gjennomsnittlig overføringshastighet for utgående trafikk. Hvis gjeldende overføringshastighet og gjennomsnittlig overføringshastighet er den samme, vises ikke den prikkete streken på diagrammet. Den heltrukne streken representerer både gjennomsnittlig og gjeldende overføringshastighet.

Analysere innkommende og utgående trafikk

Trafikkanalysediagrammet er en numerisk og grafisk representasjon av innkommende og utgående Internett-trafikk. Trafikkovervåking viser også hvilke programmer som bruker de fleste nettverkstilkoblingene på datamaskinen, og hvilke IP-adresser applikasjonene åpner.

1. Kontroller at Avansert meny er aktivert, og klikk deretter **Verktøy**.
2. I Verktøy-ruten klikker du **Trafikkovervåking**.
3. Under **Trafikkovervåking** klikker du **Trafikkanalyse**.

Tips: Hvis du vil vise den mest oppdaterte statistikken, klikker du **Oppdater** under **Trafikkanalyse**.

Overvåke båndbredden for et program

Du kan vise sektordiagrammet som viser hvor stor omtrentlig prosentandel av båndbredden som de mest aktive programmene på datamaskinen har brukt i løpet av de siste 24 timene. Sektordiagrammet gir en visuell presentasjon av den relative delen av båndbredden som brukes av programmene.

1. Kontroller at Avansert meny er aktivert, og klikk deretter **Verktøy**.
2. I Verktøy-ruten klikker du **Trafikkovervåking**.
3. Under **Trafikkovervåking** klikker du **Trafikkbruk**.

Tips: Hvis du vil vise den mest oppdaterte statistikken, klikker du **Oppdater** under **Trafikkbruk**.

Overvåke programaktivitet

Du kan vise innkommende og utgående programaktivitet, som viser tilkoblinger og porter for eksterne datamaskiner.

1. Kontroller at Avansert meny er aktivert, og klikk deretter **Verktøy**.
2. I Verktøy-ruten klikker du **Trafikkovervåking**.
3. Under **Trafikkovervåking** klikker du **Aktive programmer**.
4. Du kan vise følgende informasjon:
   - Diagram for programaktivitet: Velg et program for å vise et diagram over programmets aktivitet.
   - Lyttende tilkobling: Velg et lyttende element under programnavnet.
   - Datamaskintilkobling: Velg en IP-adresse under programnavnet, systemprosessen eller tjenesten.

Merk: Hvis du vil vise den mest oppdaterte statistikken, klikker du **Oppdater** under **Aktive programmer**.

KAPITTEL 22

Lære om Internett-sikkerhet

Firewall benytter McAfees webområde om sikkerhet, HackerWatch, til å gi oppdatert informasjon om programmer og global Internett-aktivitet. HackerWatch inneholder også en HTML-brukeropplæring om Firewall.

I dette kapitlet

Starte HackerWatch-brukeropplæringen.....122

Starte HackerWatch-brukeropplæringen

Hvis du vil lære mer om Firewall, kan du åpne HackerWatch-opplæringen fra SecurityCenter.

1. Kontroller at Avansert meny er aktivert, og klikk deretter **Verktøy**.
2. I Verktøy-ruten klikker du **HackerWatch**.
3. Under **HackerWatch Resources** (HackerWatch-ressurser) klikker du **View Tutorial** (Vis brukeropplæring).

KAPITTEL 23

McAfee Anti-Spam

Anti-Spam (tidligere kalt SpamKiller) stopper uønsket e-post fra å komme inn i innboksen din ved å kontrollere din innkommende e-post, og deretter merke den som spam (e-post som anmoder deg om å kjøpe eller phishing (e-post som anmoder deg om å oppgi personlige opplysninger til et mulig webområdehvor muligheten er stor for at det drives med svindel). Anti-Spam filtrerer spam-e-post og flytter den til McAfee Anti-Spam-mappen.

Hvis dine venner noen ganger sender deg legitim e-post som vises som spam, kan du sørge for at den ikke filtreres ved å legge deres e-postadresser til Anti-Spams venneliste. Du kan også egendefinere hvordan spam oppdages. Du kan for eksempel filtrere meldinger mer strengt, angi hva som skal sees etter i en melding og opprette dine egne filtre.

Anti-Spam beskytter deg også hvis du prøver å få tilgang til et potensielt bedragers webområde gjennom en link i en e-postmelding. Når du klikker på en link til et potensielt bedragersk webområde, blir du omdirigert til siden for phishing-filter. Hvis det finnes webområder som du ikke ønsker å filtrere, kan du legge dem til hvitelisten (webområder på denne listen filtreres ikke).

Anti-Spam er kompatibelt med flere e-postprogrammer, for eksempel POP3, POP3 Webmail, Yahoo®, MSN®/Hotmail®, Windows® Live™ Mail, og MAPI (Microsoft Exchange Server). Hvis du bruker en nettleser for å lese e-posten din må du legge til din webpostkonto til Anti-Spam. Alle andre kontoer konfigureres automatisk og du trenger ikke å legge dem til Anti-Spam.

Merknad: SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer så snart det oppdager dem. Hvis du trenger hjelp til å diagnostisere beskyttelsesproblemene, kan du kjøre McAfee Virtual Technician.

I dette kapitlet

Anti-Spam-funksjoner 125
Konfigurere webpostkontoer 127
Konfigurere venner 131
Konfigurere spamoppdagelse 137
E-postfiltrering 145
Arbeide med filtrert e-post 149
Konfigurere beskyttelse mot phishing 151

Anti-Spam-funksjoner

Anti-Spam har følgende funksjoner.

Spamfiltrering

Anti-Spams avanserte filtre forhindrer at uønsket e-post fra å komme inn i innboksen din, og oppdateres automatisk for alle dine e-postkontoer. Du kan også opprette egendefinerte filtre for å påse at all spam filtreres, og rapportere spam til McAfee for analysering.

Phishing-filtrering

Phishing-filteret identifiserer potensielle phishing (bedragerske)-webområder som ber om personlig informasjon.

Egendefinert spam-behandling

Merk uønsket e-post som spam og flytt den til McAfee Anti-Spam-mappen, eller merk legitim e-post som ikke er spam og flytt den til innboksen.

Venner

Importer dine venners e-postadresser til vennelisten slik at deres e-postmeldinger ikke filtreres.

Sorter listeelementer etter relevans

Du kan sortere dine personlige filtre, venner, adresserbøker og webpostkontoer etter relevans (klikk på det passende kolonnenavnet).

Ekstra støtte

Anti-Spam støtter Mozilla® Thunderbird™ 1.5 and 2.0, og gir Windows Vista™ 64-bit støtte for Windows Mail. I tillegg stopper den nye spillemodusfunksjonen Anti-Spam-bakgrunnsprosesser slik at din datamaskin ikke går mer sakte mens du spiller videospill eller ser på DVD-er. Anti-Spam filtrere også Microsoft® Outlook®, Outlook Express eller Windows Mail-kontoer på alle porter, inkludert SSL-porter (Secure Socket Layer).

KAPITTEL 24

Konfigurere webpostkontoer

Hvis du bruker en nettleser for å lese dine e-postmeldinger, må du konfigurere Anti-Spam til å kobles til din konto og filtrere dine meldinger. For å legge din webpostkonto til Anti-Spam, legger du til kontoinformasjonen gitt av din e-postleverandør.

Etter at du har lagt til en webpostkonto, kan du redigere kontoinformasjonen og få mer informasjon om filtrering av webpost. Hvis du ikke lenger bruker en webpostkonto, eller du ikke ønsker at den filtreres, kan du fjerne den.

Anti-Spam er kompatibelt med flere e-postprogrammer, for eksempel POP3, POP3 Webmail, Yahoo®, MSN/Hotmail, Windows Live Mail, og MAPI-kontoer POP3e er den vanligste kontotypen. Den er standard for Internett-e-post. Når du har en POP3-konto, kobler Anti-Spam seg direkte til e-postserveren og filtrerer meldingene før de hentes av e-postprogrammet. POP3 Webmail, Yahoo, MSN/Hotmail og Windows Mail-kontoer er webbaserte. Filtrering av POP3-webpostkontoer fungerer på samme måte som filtrering av POP3-kontoer. MAPI er et system som er utviklet av Microsoft. Det støtter mange typer meldinger, inkludert Internett-e-post, faks og meldinger via Exhange-tjener. For øyeblikket kan kun Microsoft Oultook arbeide direkte med MAPI-kontoer.

Merknad: Selv om Anti-Spam kan aksessere MAPI-kontoer, filtrerer det ikke e-posten din før du har hentet frem meldingene dine med Microsoft Outlook.

I dette kapitlet

Legge til en webpostkonto.....127
Redigere en webpostkonto.....128
Fjerne en webpostkonto.....129
Forstå webpostkontoinformasjon.....129

Legge til en webpostkonto

Legg til en POP3 (for eksempel, Yahoo), MSN/Hotmail, eller Windows Mail (kun betalte versjoner støttes helt) webpostkonto.

1 Åpne ruten Spam-beskyttelse.

Hvordan?

1. Klikk **E-post og direktemeldinger** i Hjem-ruten til SecurityCenter.
2. Klikk på **Konfigurer** i informasjonsområdet for E-post og direktemeldinger.
3. Klikk på **Avansert** i ruten Konfigurasjon av e-post og direktemeldinger under **Spambeskyttelse**.

2 Klikk **Webpostkontoer** i ruten Spambeskyttelse.

3 Klikk **Legg til** i ruten Webpostkontoer.

4 Angi kontoinformasjon (side 129), og klikk deretter på **Neste**.

5 Under **Alternativer for sjekking** angir dunår Anti-Spam kontrollerer din konto for spam (side 129).

6 Hvis du bruker oppringt tilkobling, angir du hvordan Anti-Spam kobler til Internett (side 129).

7 Klikk på **Fullfør**.

Redigere en webpostkonto

Du må redigere webpostkontoinformasjonen når endringer for kontoen din oppstår. Rediger for eksempel webpostkontoen hvis du har endret passordet eller hvis du vil at Anti-Spam skal kotrollere oftere for spam.

1 Åpne ruten Spam-beskyttelse.

Hvordan?

1. Klikk **E-post og direktemeldinger** i Hjem-ruten til SecurityCenter.
2. Klikk på **Konfigurer** i informasjonsområdet for E-post og direktemeldinger.
3. Klikk på **Avansert** i ruten Konfigurasjon av e-post og direktemeldinger under **Spambeskyttelse**.

2 Klikk **Webpostkontoer** i ruten Spambeskyttelse.

3 Velg kontoen du vil endre, og klikk **Rediger**.

4 Angi kontoinformasjon (side 129), og klikk deretter på **Neste**.

5 Under **Alternativer for sjekking** angir dunår Anti-Spam kontrollerer din konto for spam (side 129).

6 Hvis du bruker oppringt tilkobling, angir du hvordan Anti-Spam kobler til Internett (side 129).

7 Klikk på **Fullfør**.

Fjerne en webpostkonto

Fjern en webpostkonto hvis du ikke lenger vil filtrere e-posten for spam. Hvis kontoen din for eksempel ikke er aktiv lenger og du erfarer problemer kan du fjerne kontoen mens du feilsøker for problemet.

1 Åpne ruten Spam-beskyttelse.

Hvordan?

1. Klikk **E-post og direktemeldinger** i Hjem-ruten til SecurityCenter.
2. Klikk på **Konfigurer** i informasjonsområdet for E-post og direktemeldinger.
3. Klikk på **Avansert** i ruten Konfigurasjon av e-post og direktemeldinger under **Spambeskyttelse**.

2 Klikk **Webpostkontoer** i ruten Spambeskyttelse.

3 Velg kontoen du vil fjerne, og klikk **Fjern**.

Forstå webpostkontoinformasjon

Den følgende tabellen beskriver informasjonen du må angi når du legger til eller rediere webpostkontoer.

Kontoopplysninger

Informasjon	Beskrivelse
Beskrivelse	Beskriv kontoen for egen referanse. I denne boksen kan du skrive inn den informasjonen du ønsker.
E-postadresse	Angi e-postadresser tilknyttet denne e-postkontoen.
Kontotype	Angi typen e-postkonto du legger til. (for eksempel, POP3 eller MSN/Hotmail).
Tjener	Angir navnet på mailserveren som er vert for denne kontoen. Hvis du ikke kjenner servernavnet, henvises det til informasjonen fra din tjenestetilbyder for Internett (ISP).
Brukernavn	Angi brukernavnet for denne e-postkontoen. Hvis e-postadressen din for eksempel er *brukernavn*@hotmail.com, vil brukernavnet sannsynligvis være *brukernavn*.
Passord	Angi passordet for denne e-postkontoen.
Bekreft passord	Bekreft passordet for denne e-postkontoen.

Alternativer for sjekking

Alternativer	Beskrivelse
Kontroller hvert	Anti-Spam sjekker denne kontoen for spam i henhold til intervallet (antall minutter) du angir. Intervallene må være mellom 5 og 3600 minutter.
Kontroller ved oppstart	Anti-Spam sjekker kontoen hver gang du starter datamaskinen på nytt.

Tilkoblingsalternativer

Alternativer	Beskrivelse
Ring aldri opp en tilkobling	Anti-Spam ringer ikke automatisk opp en tilkobling for deg. Du må starte den oppringte tilkoblingen manuelt.
Ring opp når ingen tilkobling er tilgjengelig	Når ingen Internett-tilkobling er tilgjengelig, prøver Anti-Spam å koble til ved hjelp av den oppringte tilkoblingen du angir.
Ring alltid opp den angitte tilkoblingen	Anti-Spam prøver å koble til ved hjelp av den oppringte tilkoblingen du angir. Hvis du er koblet til via en anne oppringt tilkobling enn den du oppgir, vil du kobles fra.
Ring opp denne tilkoblingen	Angi den oppringte tilkoblingen Anti-Spam bruker for å koble til Internett.
Behold forbindelse etter at filtrering er fullført	Datamaskinen beholder forbindelsen til Internett etter at filtreringen er fullført.

KAPITTEL 25

Konfigurere venner

For å sikre at Anti-Spam ikke filtrere legitime e-postmeldinger fra dine venner kan du legge til deres adresser til Anti-Spams venneliste.

Den enkleste måten for å oppdatere vennelisten er å legge adressebøkene dine til Anti-Spam, slik at alle dine venners e-postadresser importeres. Etter at du har lagt til en adressebok, importeres innholdet automatisk til bestemte intervaller (daglig, ukentlig eller månedlig) for å forhindre at vennelisten ikke holdes oppdatert.

Du kan også oppdatere Anti-Spams venneliste manuelt, eller legge til et helt domene hvis du ønsker at hver bruker på det domenet skal legges til vennelisten. Du kan for eksempel legge til bedriften.com domene, og ingen av e-postene fra den organisasjonen filtreres.

I dette kapitlet

Konfigurere venner automatisk 132
Konfigurere venner automatisk 134

Konfigurere venner automatisk

Du kan automatisk oppdatere vennelisten ved å legge til adressebøker til Anti-Spam. Hvis du legger til en adressebok til Anti-Spam kan de tilknyttede e-postadressene importeres og tilføres vennelisten.

Etter at du har lagt til en adresserbok kan du endre hvor ofte innholdet skal importeres til vennelisten. Du kan også fjerne en adressebok hvis du ikke lenger ønsker å importere innholdet i den.

Legge til en adressebok

Legg til dine adressebøker slik at Anti-Spam automatisk kan importere alle dine e-postadresser og oppdatere vennelisten. Dette sørger for at din venneliste alltid er oppdatert.

1 Åpne ruten Spam-beskyttelse.

   Hvordan?

   1. Klikk **E-post og direktemeldinger** i Hjem-ruten til SecurityCenter.
   2. Klikk på **Konfigurer** i informasjonsområdet for E-post og direktemeldinger.
   3. Klikk på **Avansert** i ruten Konfigurasjon av e-post og direktemeldinger under **Spambeskyttelse**.

2 Klikk **Adressebøker** i ruten Spambeskyttelse.

3 Klikk **Legg til** i ruten Adressebøker.

4 Klikk typen adressebok du vil importere, i listen **Type**.

5 Hvis listen **Kilde** er fylt ut, velg adressebokkilden. Hvis du for eksempel har en Outlook-adressebok må du velge Outlook fra denne listen.

6 Klikk **Daglig, Ukentlig** eller **Månedlig** i listen **Tidsplan** for å angi når AntiSpam skal sjekke om adresseboken inneholder nye adresser.

7 Klikk **OK**.

Redigere en adressebok

Når du har lagt til adressebøker kan du endre importinformasjonen og tidsplanen for dem. Du kan for eksempel redigere dine adressebøker hvis du vil at Anti-Spam skal kontrollere oftere for nye adresser.

1 Åpne ruten Spam-beskyttelse.

   Hvordan?

1. Klikk **E-post og direktemeldinger** i Hjem-ruten til SecurityCenter.
2. Klikk på **Konfigurer** i informasjonsområdet for E-post og direktemeldinger.
3. Klikk på **Avansert** i ruten Konfigurasjon av e-post og direktemeldinger under **Spambeskyttelse**.

2 Klikk **Adressebøker** i ruten Spambeskyttelse.

3 Velg adresseboken du vil redigere, og klikk **Rediger**.

4 Klikk typen adressebok du vil importere, i listen **Type**.

5 Hvis listen **Kilde** er fylt ut, velg adressebokkilden. Hvis du for eksempel har en Outlook-adressebok må du velge Outlook fra denne listen.

6 Klikk **Daglig, Ukentlig** eller **Månedlig** i listen **Tidsplan** for å angi når AntiSpam skal sjekke om adresseboken inneholder nye adresser.

7 Klikk **OK**.

Fjerne en adressebok

Fjern en adressebok når du ikke lenger ønsker at Anti-Spam automatisk skal importere adresser fra den (hvis en adressebok for eksempel er utdatert og du ikke ønsker å bruke den lenger).

1 Åpne ruten Spam-beskyttelse.

Hvordan?

1. Klikk **E-post og direktemeldinger** i Hjem-ruten til SecurityCenter.
2. Klikk på **Konfigurer** i informasjonsområdet for E-post og direktemeldinger.
3. Klikk på **Avansert** i ruten Konfigurasjon av e-post og direktemeldinger under **Spambeskyttelse**.

2 Klikk **Adressebøker** i ruten Spambeskyttelse.

3 Velg adresseboken du vil fjerne, og klikk **Fjern**.

Konfigurere venner automatisk

Du oppdaterer vennelisten manuelt med å redigere en og en oppføring. Hvis du for eksempel mottar en e-post fra en venn og adressen ikke er i adresseboken, kan du manuelt legge til e-postadressen med en gang. Den enkleste måten å gjøre dette på er å bruke verktøylinjen for Anti-Spam. Hvis du ikke bruker Anti-Spam-verktøylinje må du angi informasjonen om vennene dine.

Legge til en venn fra Anti-Spam-verktøylinjen

Hvis du bruker Outlook, Outlook Express, Windows Mail, Eudora eller Thunderbird som e-postprogram, kan du legge til venner direkte fra Anti-Spam-verktøylinjen.

Legg til en venn i...	Velg en melding, og...
Outlook, Outlook Express, Windows Mail	Klikk på **Legg til venn**.
Eudora, Thunderbird	På **Anti-Spam**-menyen klikker du deretter **Legg til venn**.

Legg til en venn manuelt

Hvis du ikke ønsker å legge til en venn direkte fra verktøylinjen, eller du glemte å gjøre det når du mottok e-postmeldingen, kan du fremdeles legge en venn til vennelisten uten å vente på at Anti-Spam automatisk skal importere adresseboken.

1. Åpne ruten Spam-beskyttelse.

   Hvordan?

   1. Klikk **E-post og direktemeldinger** i Hjem-ruten til SecurityCenter.
   2. Klikk på **Konfigurer** i informasjonsområdet for E-post og direktemeldinger.
   3. Klikk på **Avansert** i ruten Konfigurasjon av e-post og direktemeldinger under **Spambeskyttelse**.

2. Klikk **Venner** i ruten Spambeskyttelse.
3. Klikk **Legg til** i ruten Venner.
4. Skriv inn navnet på vennen i boksen **Navn**.
5. Velg **Enkel e-postadresse**i listen **Type** list.
6. Skriv inn din venns e-postadresse i boksen **E-postadresse**.
7. Klikk **OK**.

Legg til et domene

Legg til et helt domene hvis du ønsker å legge til hver eneste bruker på det domene til vennelisten. Du kan for eksempel legge til bedriften.com domene, og ingen av e-postene fra den organisasjonen filtreres.

1 Åpne ruten Spam-beskyttelse.

   Hvordan?

   1. Klikk **E-post og direktemeldinger** i Hjem-ruten til SecurityCenter.
   2. Klikk på **Konfigurer** i informasjonsområdet for E-post og direktemeldinger.
   3. Klikk på **Avansert** i ruten Konfigurasjon av e-post og direktemeldinger under **Spambeskyttelse**.

2 Klikk **Venner** i ruten Spambeskyttelse.

3 Klikk **Legg til** i ruten Venner.

4 Skriv inn navnet på organisasjonen eller gruppen i boksen **Navn**.

5 Velg **Helt domene** i listen **Type** .

6 Skriv inn domenenavnet i boksen **E-postadresse**.

7 Klikk **OK**.

Rediger en venn

Hvis informasjonen om en venn endres, kan du oppdatere listen din for å forsikre deg om at Anti-Spam ikke merker deres meldinger som spam.

1 Åpne ruten Spam-beskyttelse.

   Hvordan?

   1. Klikk **E-post og direktemeldinger** i Hjem-ruten til SecurityCenter.
   2. Klikk på **Konfigurer** i informasjonsområdet for E-post og direktemeldinger.
   3. Klikk på **Avansert** i ruten Konfigurasjon av e-post og direktemeldinger under **Spambeskyttelse**.

2 Klikk **Venner** i ruten Spambeskyttelse.

3 Velg vennen du vil redigere, og klikk **Rediger**.

4 Endre navnet på vennen i boksen **Navn**.

5 Endre din venns e-postadresse i boksen **E-postadresse**.

6 Klikk **OK**.

Redigere et domene

Hvis informasjonen for et domene endres, kan du oppdatere listen din for å forsikre deg om at Anti-Spam ikke merker deres meldinger som spam.

1 Åpne ruten Spam-beskyttelse.

   Hvordan?

   1. Klikk **E-post og direktemeldinger** i Hjem-ruten til SecurityCenter.
   2. Klikk på **Konfigurer** i informasjonsområdet for E-post og direktemeldinger.
   3. Klikk på **Avansert** i ruten Konfigurasjon av e-post og direktemeldinger under **Spambeskyttelse**.

2 Klikk **Venner** i ruten Spambeskyttelse.

3 Klikk **Legg til** i ruten Venner.

4 Endre navnet på organisasjonen eller gruppen i boksen **Navn**.

5 Velg **Helt domene** i listen **Type** .

6 Endre domenenavnet i boksen **E-postadresse**.

7 Klikk **OK**.

Fjerne en venn

Hvis en person eller et domene i vennelisten sender deg spam kan du fjerne dem fra Anti-Spams venneliste slik at deres e-postmeldinger filtreres igjen.

1 Åpne ruten Spam-beskyttelse.

   Hvordan?

   1. Klikk **E-post og direktemeldinger** i Hjem-ruten til SecurityCenter.
   2. Klikk på **Konfigurer** i informasjonsområdet for E-post og direktemeldinger.
   3. Klikk på **Avansert** i ruten Konfigurasjon av e-post og direktemeldinger under **Spambeskyttelse**.

2 Klikk **Venner** i ruten Spambeskyttelse.

3 Velg vennen du vil fjerne, og klikk **Fjern**.

KAPITTEL 26

Konfigurere spamoppdagelse

Med Anti-Spam kan du egendefinere hvordan spam skal oppdages. Du kan filtrere meldingene strengere, angi hva som skal sees etter i en melding og se etter bestemte tegnoppsett ved analysering a spam. Du kan også opprette personlige filtre for å finjustere hvilke meldinger Anti-Spam skal gjenkjenne som spam. Hvis for eksempel uønsket e-post som inneholder ordet lån ikke filtreres, kan du legget til et filter som inneholder ordet lån.

Hvis du har problemer med din e-post kan du deaktivere spambeskyttelsen som en del av feilsøkingsmetoden.

I dette kapitlet

Deaktivere spambeskyttelse.....137
Definere filtreringsalternativer 138
Bruke personlige filtre.....141

Deaktivere spambeskyttelse

Hvis du vil forhindre at Anti-Spam filtrerer e-post, kan du deaktivere spambeskyttelse.

1. Klikk **Konfigurer** på den avanserte menyen.
2. Klikk **E-post og direktemeldinger** i ruten Konfigurer.
3. Under **Spambeskyttelse** klikker du **Av**.

Tips: Husk å klikke **På** under **Spambeskyttelse** slik at du er beskyttet mot spam.

Definere filtreringsalternativer

Juster filtreringsalternativene for Anti-Spam hvis du vil filtrere meldingene strengere, angi hva som skal sees etter i en melding og se etter bestemte tegnoppsett ved analysering a spam.

Filtreringsnivå

Filtreringsnivået angir hvor sterkt e-posten filtreres. Hvis spam ikke filtreres og filtreringsnivået er satt til Medium, kan du endre det til Høyt. Hvis filtreringsnivået er satt til Høyt vil kun e-postadresser fra avsendere som er oppført i vennelisten aksepteres: alle andre meldinger filtreres.

Spesialfiltre

Et filter angir hva Anti-Spam ser etter i en e-postmelding. Spesialfiltre oppdager e-postmeldinger som inneholder skjult tekst, innføyde bilder, bevisste HTML-formatteringsfeil og andre teknikker som vanligvis brukes av spammere. E-postmeldinger som har disse kjennetegnene er vanligvis spam, og spesialfiltre aktiveres dermed som standard. Hvis du for eksempel ønsker å motta e-postmeldinger som inneholder innføyde bilder, må du deaktivere det spesielle bildefilteret.

Tegnsett

Anti-Spam kan se etter bestemte tegnsett under analysering av spam. Tegnsett inneholder blant annet et språks alfabet, tall og andre symboler. Hvis du mottar spam på gresk kan du filtrere alle meldinger som inneholder det greske tegnsettet.

Ikke filtrer tegnsett for språk som du mottar legitim e-post på. Hvis du kun ønsker å filtrere meldinger på italiensk kan du velge vest-europeisk fordi Italia er i Vest-Europa. Hvis du mottar en legitim e-post på engelsk, vil valget av vest-europeisk også filtrere meldinger på engelsk og andre språk i det vest-europeiske tegnspråket. I dette tilfellet kan du ikke bare filtrere meldinger på italiensk.

Merk: Filtrering av meldinger som inneholder tegn fra et bestemt tegnsett bør utføres av avanserte brukere.

Endre filtreringsnivået

Du kan endre hvor strengt du vil filtrere dine e-postmeldinger. Hvis for eksempel legitime meldinger blir filtrert, kan du endre til et lavere filtreringsnivå.

1 Åpne ruten Spam-beskyttelse.

Hvordan?

1. Klikk **E-post og direktemeldinger** i Hjem-ruten til SecurityCenter.
2. Klikk på **Konfigurer** i informasjonsområdet for E-post og direktemeldinger.
3. Klikk på **Avansert** i ruten Konfigurasjon av e-post og direktemeldinger under **Spambeskyttelse**.

2 Klikk **Filtreringsalternativer** i ruten Spambeskyttelse.

3 Under **Filtreringsalternativer** flytter du glidebryteren til det passende nivået og klikker **OK**.

Nivå	Beskrivelse
Svakt	De fleste e-postmeldinger godtas.
Middels lavt	Bare åpenbare spammeldinger filtreres.
Middels	E-post filtreres til det anbefalte nivået.
Middels høyt	Alle e-postmeldinger som ligner spam, filtreres.
Høy	Bare meldinger fra avsendere i vennelisten din godkjennes.

Deaktivere et spesialfilter

Spesialfiltre aktiveres som standardinnstilling fordi de filtrerer meldinger som spammere vanligvis sender. E-postmeldinger som inneholder innføyde bilder er vanligvis spam, men hvis du ofte mottar legitim e-post med bildevedlegg bør du deaktivere det spesielle bildefilteret.

1 Åpne ruten Spam-beskyttelse.

Hvordan?

1. Klikk **E-post og direktemeldinger** i Hjem-ruten til SecurityCenter.
2. Klikk på **Konfigurer** i informasjonsområdet for E-post og direktemeldinger.
3. Klikk på **Avansert** i ruten Konfigurasjon av e-post og direktemeldinger under **Spambeskyttelse**.

2 Klikk **Filtreringsalternativer** i ruten Spambeskyttelse.

3 Under **Spesialfiltre** setter du inn eller fjerner merket i korrekte avmerkingsbokser og klikker **OK**.

Filter	Beskrivelse
Filtrer meldinger som inneholder skjult tekst	Ser etter skjult tekst fordi meldinger med skjult tekst ofte brukes av spammere for å unngå at de oppdages.

Filtrer meldinger som inneholder spesielle forhold mellom bilder og tekst	Ser etter innføyde bilder fordi meldinger med innføyde bilder vanligvis er spam.
Filtrer meldinger som inneholder tilsiktede HTML-formateringsfeil	Ser etter meldinger som inneholder ugyldig formatering, fordi ugyldig formatering brukes til å forhindre filtre fra å filtrere spam.
Ikke filtrer meldinger større enn	Ser ikke etter meldinger som er større enn den angitte størrelsen fordi større meldinger muligens ikke er spam. Du kan øke eller redusere meldingsstørrelsen (gyldig intervall er 0-250 kB).

Ta i bruk filtre for tegnsett

Merk: Filtrering av meldinger som inneholder tegn fra et bestemt tegnsett bør utføres av avanserte brukere.

Du kan filtrere bestemte språktegnsett, men ikke filtrer tegnsett for språk som du mottar legitim e-post på.

1 Åpne ruten Spam-beskyttelse.

Hvordan?

1. Klikk **E-post og direktemeldinger** i Hjem-ruten til SecurityCenter.
2. Klikk på **Konfigurer** i informasjonsområdet for E-post og direktemeldinger.
3. Klikk på **Avansert** i ruten Konfigurasjon av e-post og direktemeldinger under **Spambeskyttelse**.

2 Klikk **Tegnsett** i ruten Spambeskyttelse.

3 Merk av i boksene ved siden av tegnsettene du vil filtrere.

4 Klikk **OK**.

Bruke personlige filtre

Et filter angir hva Anti-Spam ser etter i en e-postmelding. Når spam finnes merkes meldingen som spam og blir liggende i innboksen eller flyttet til McAffe Anti-Spam-mappe. Du finner mer informasjon om hvordan spam håndteres på Endre hvordan en melding behandles og merkes (side 146).

Anti-Spam bruker mange filtre. Du kan imidlertid opprette nye filtre eller redigere eksisterende filtre for å finjustere hvilke meldinger Anti-Spam identifiseres som spam. Du kan for eksempel legge til et filter som inneholder ordet lån, og Anti-Spam vi filtrere meldinger med ordet lån. Ikke opprett filtre for vanlige ord som forekommer i legitime e-postmeldinger. Da vil til og med e-post som ikke er spam bli filtrert. Når du har opprettet et filter, kan du redigere det hvis du finner ut at filteret ikke oppdager spam. Du kan for eksempel ha opprettet et filter som skal se etter ordet viagra i emnefeltet på meldingen, men du mottar fremdeles meldinger som inneholder ordet viagra fordi det vises i selve meldingen. Du kan da endre filteret til å se etter ordet viagra i selve meldingen i stedet for i emnefeltet.

Vanlige uttrykk (RegEx) er spesialtegn og sekvenser som også kan brukes i personlig filtre, men McAfee anbefaler kun bruk av vanlige uttrykk hvis du er en erfaren bruker. Hvis du ikke er kjent med vanlige uttrykk, eller du ønsker mer informasjon om hvordan å bruke dem, kan du søke etter vanglige uttrykk på Internett (du kan for eksempel gå til http://en.wikipedia.org/wiki/Regular_expression).

Legg til et personlig filter

Du kan legge til filtre for å finjustere hvilke meldinger Anti-Spam identifiserer som spam.

1. Åpne ruten for beskyttelse mot spam.

   Hvordan?

   1. Klikk **E-post og direktemeldinger** i Hjem-ruten til SecurityCenter.
   2. Klikk på **Konfigurer** i informasjonsområdet for E-post og direktemeldinger.
   3. Klikk på **Avansert** i ruten Konfigurasjon av e-post og direktemeldinger under **Spambeskyttelse**.

2. Klikk **Personlige filtre** i ruten Spambeskyttelse.
3. Klikk på **Legg til**.
4. Angi hva det personlige filteret ser etter (side 142) i en e-postmelding.
5. Klikk **OK**.

Rediger et personlig filter

Rediger eksisterende filtre for å finjustere hvilke meldinger som blir identifisert som spam.

1 Åpne ruten for beskyttelse mot spam.

   Hvordan?

   1. Klikk **E-post og direktemeldinger** i Hjem-ruten til SecurityCenter.
   2. Klikk på **Konfigurer** i informasjonsområdet for E-post og direktemeldinger.
   3. Klikk på **Avansert** i ruten Konfigurasjon av e-post og direktemeldinger under **Spambeskyttelse**.

2 Klikk **Personlige filtre** i ruten Spambeskyttelse.

3 Velg filteret du vil redigere, og klikk **Rediger**.

4 Angi hva det personlige filteret ser etter (side 142) i en e-postmelding.

5 Klikk **OK**.

Fjerne et personlig filter

Du kan permanent fjerne filtre du ikke lenger vil bruke.

1 Åpne ruten for beskyttelse mot spam.

   Hvordan?

   1. Klikk **E-post og direktemeldinger** i Hjem-ruten til SecurityCenter.
   2. Klikk på **Konfigurer** i informasjonsområdet for E-post og direktemeldinger.
   3. Klikk på **Avansert** i ruten Konfigurasjon av e-post og direktemeldinger under **Spambeskyttelse**.

2 Klikk **Personlige filtre** i ruten Spambeskyttelse.

3 Velg filteret du vil fjerne, og klikk **Fjern**.

4 Klikk **OK**.

Spesifisering av personlig filter

Følgene tabell beskriver hva et personlig filter ser etter i en e-postmelding.

Informasjon	Beskrivelse
Element	Klikk en oppføring for å fastslå om filteret skal se etter ord eller fraser i emnelinjen, meldingsteksten, hoder eller avsender.
Vilkår	Klikk en oppføring for å fastslå om filteret skal se etter meldinger som inneholder, eller ikke inneholder, ordene eller frasene du angir.

Ord eller fraser	Skriv hva det skal søkes etter i en melding. Hvis du for eksempel angir forbrukslån, filtreres alle meldinger som inneholder dette ordet.
Dette filteret bruker vanlige uttrykk (RegEx)	Angi tegnmønstre brukt i filtreringsvilkår. Hvis du vil teste et tegnmønster, klikker du **Test**.

KAPITTEL 27

E-postfiltrering

Anti-Spam undersøker din innkommende e-post, og kategoriserer den som spam (e-post som anmoder deg om å kjøpe), eller phishing (e-post som anmoder deg om å oppgi personlige opplysninger til kjente eller potensielt bedragerske webområder). Anti-Spam merker som standard enhver uønsket e-postmelding som spam eller phishing (taggen [SPAM] eller [PHISH] vises i emnelinjen til meldingen), og flytter meldingen til McAfee Anti-Spam mappen.

Du kan tilpasse måten Anti-Spam filtrerer dine e-postmeldinger, ved å merke e-post som spam eller ikke spam fra Anti-Spam verktøylinjen, endre plasseringen hvor spammeldinger blir flyttet, eller endre taggen som vises i emnelinjen.

Du kan endre hvordan spam behandles og merkes, tilpasse lokaliseringen hvor spam og phishing-epostmeldinger blir flyttet, og tilpasse navnet på taggen som vises i emnelinjen.

Du kan også deaktivere Anti-Spam-verktøylinjer som del av din feilsøkingsmetode når du har problemer med ditt e-postprogram.

I dette kapitlet

Merk en melding fra Anti-Spam verktøylinjen.....145
Modifiser hvordan en melding blir behandlet og merket 146
Deaktiver Anti-Spam-verktøylinjen.....146

Merk en melding fra Anti-Spam verktøylinjen

Når du merker en melding som spam, tagges emnet i meldingen med [SPAM] eller en egendefinert tagg og blir liggende i din innboks, din McAfee Anti-Spam mappe (Outlook, Outlook Express, Windows Mail, Thunderbird) eller din mappe for søppelpost (Eudora®). Når du merker en melding som ikke spam, blir meldingstaggen fjernet, og meldingen flyttet til innboksen.

For å merke en melding i...	Velg en melding, og klikk deretter...
Outlook, Outlook Express, Windows Mail	Klikk på **Merk som spam** eller **Merk som ikke spam**.
Eudora, Thunderbird	På **Anti-Spam**-menyen klikker du **Merk som spam** eller **Merk som ikke spam.**

Modifiser hvordan en melding blir behandlet og merket

Du kan endre endre hvordan spam behandles og merkes. For eksempel kan du bestemme hvorvidt e-postmeldingen blir igjen i din innboks eller McAfee Anti-Spam mappe, og endre [SPAM] eller [PHISH] taggen som vises i emnelinjen i meldingen.

1 Åpne ruten for beskyttelse mot spam.

Hvordan?

1. Klikk **E-post og direktemeldinger** i Hjem-ruten til SecurityCenter.
2. Klikk på **Konfigurer** i informasjonsområdet for E-post og direktemeldinger.
3. Klikk på **Avansert** i ruten Konfigurasjon av e-post og direktemeldinger under **Spambeskyttelse**.

2 Klikk **Behandling** i ruten Spambeskyttelse.

3 Velg eller fjern de riktige avmerkingsboksene, og klikk så **OK**.

Alternativer	Beskrivelse
Merk som spam og flytt til McAfee Anti-Spam mappen.	Dette er standardinnstillingen. Spammeldinger flyttes til din McAfee Anti-Spam mappe.
Merk som spam og la dem bli i innboksen	Spammeldinger blir liggende i innboksen.
Legg til denne egendefinerbare taggen i emnet til spammeldinger	Taggen du angir, legges til i emnet på spammeldinger.
Legg til denne egendefinerbare taggen i emnet til phishing-meldinger	Taggen du angir, legges til i emnet på phishing-meldinger.

Deaktiver Anti-Spam-verktøylinjen

Hvis du bruker Outlook, Outlook Express, Windows Mail, Eudora eller Thunderbird, kan du deaktivere Anti-Spam-verktøylinjen.

1 Åpne ruten for beskyttelse mot spam.

Hvordan?

1. Klikk **E-post og direktemeldinger** i Hjem-ruten til SecurityCenter.
2. Klikk på **Konfigurer** i informasjonsområdet for E-post og direktemeldinger.
3. Klikk på **Avansert** i ruten Konfigurasjon av e-post og direktemeldinger under **Spambeskyttelse**.

2 Klikk **E-postverktøylinjer** i ruten Spambeskyttelse.

3 Fjern merket i avmerkingsboksen ved siden av kontoen du vil deaktivere.

4 Klikk **OK**.

Tips: Du kan reaktivere dine Anti-Spam-verktøylinjer når som helst ved å velge deres avmerkingsbokser.

KAPITTEL 28

Arbeide med filtrert e-post

Til tider kan det hende at noe spam ikke bli oppdaget. Når dette hender, kan du rapportere spam til McAfee, hvor det blir analysert for å lage filteroppdateringer.

Hvis du bruker en webpostkonto, kan du kopiere, slette, og motta mer informasjon om dine filtrerte e-postmeldinger. Detter er nyttig når du ikke er sikker på hvorvidt en legitim melding ble filtrert, eller hvis du ønsker å vite når meldingen ble filtrert.

I dette kapitlet

Rapportere spam til McAfee 149
Kopier eller slett en filtrert webpostmelding..... 150
Vis en hendelse for filtrert webpost 150

Rapportere spam til McAfee

Du kan rapportere spam til McAfee, hvor det blir analysert for å lage filteroppdateringer.

1 Åpne ruten for beskyttelse mot spam.

   Hvordan?

   1. Klikk **E-post og direktemeldinger** i Hjem-ruten til SecurityCenter.
   2. Klikk på **Konfigurer** i informasjonsområdet for E-post og direktemeldinger.
   3. Klikk på **Avansert** i ruten Konfigurasjon av e-post og direktemeldinger under **Spambeskyttelse**.

2 Klikk **Rapporter til McAfee** i ruten Spambeskyttelse.

3 Velg riktig avmerkingsboks, og klikk så **OK**.

Alternativer	Beskrivelse
Aktiver rapportering når du klikker Merk som spam	Rapporterer en melding til McAfee hver gang du merker den som spam.
Aktiver rapportering når du klikker Merk som ikke spam	Rapporterer en melding til McAfee hver gang du merker den som ikke spam.
Send hele meldingen (ikke bare hoder)	Sender hele meldingen, ikke bare hodene, når du rapporterer en melding til McAfee.

Kopier eller slett en filtrert webpostmelding

Du kan kopiere eller slette meldinger som er filtrert i webpostkontoen din.

1. Under **Vanlige oppgaver,** klikk på **Se nylige hendelser**.
2. Klikk **Vis logg** i ruten Nylige hendelser.
3. Utvid listen **E-post og direktemeldinger** i venstre rute, og klikk **Webpostfiltreringshendelser**.
4. Velg en melding
5. Under **Jeg vil** gjør du ett av følgende:
   - Klikk **Kopier** for å kopiere meldingen til utklippstavlen.
   - Klikk **Slett** for å slette meldingen.

Vis en hendelse for filtrert webpost

Du kan se datoen og tiden da e-postmeldingene ble filtrert og kontoen som mottok dem.

1. Under **Vanlige oppgaver,** klikk på **Se nylige hendelser**.
2. Klikk **Vis logg** i ruten Nylige hendelser.
3. Utvid listen **E-post og direktemeldinger** i venstre rute, og klikk **Webpostfiltreringshendelser**.
4. Velg loggen du vil vise.

KAPITTEL 29

Konfigurere beskyttelse mot phishing

Anti-Spam kategoriserer uønsket e-post som spam (e-post som anmoder deg om å kjøpe), eller phishing (e-post som anmoder deg om å oppgi personlige opplysninger til kjente eller potensielt bedragerske webområder). Beskyttelse mot phishing beskytter deg mot tilgang til bedragerske webområder. Hvis du klikker på en lenke i en e-postmelding til en kjent eller potensielt bedragersk webområder, vil Anti-Spam omdirigere deg til den sikre siden for phishing-filter.

Hvis det er webområder som du ønsker å filtrere, legg disse til hvitelisten for phishing. Du kan også redigere eller fjerne webområder fra hvitelisten. Du trenger ikke å legge til sider som Google®, Yahoo, or McAfee, fordi disse webområder ikke anses som bedragerske.

Merk: Hvis du har SiteAdvisor installert, vil du ikke motta beskyttelse mot phishing fra Anti-Spam fordi SiteAdvisor allerede har en lignende beskyttelse mot phishing.

I dette kapitlet

Legge et webområdet til hvitelisten 151
Rediger områder i din hviteliste 152
Fjerne et webområde fra hvitelisten 152
Deaktivere beskyttelse mot phishing..... 152

Legge et webområdet til hvitelisten

Hvis det er webområder som du ønsker å filtrere, legg disse til hvitelisten.

1. Åpne ruten for beskyttelse mot phishing

   Hvordan?

   1. I Hjem-ruten for SecurityCenter klikker du **Internett og & nettverk.**
   2. I informasjonsområdet & for Internett og nettverk klikker du**Konfigurer**.

2. I ruten for beskyttelse mot phishing, klikk på **Avansert**.
3. Under **Hviteliste,** klikk **Legg til.**
4. Skriv inn adressen til webområdet, og klikk deretter **OK**.

Rediger områder i din hviteliste

Dersom du la til et webområde til hvitelisten og adressen til webområdet endres, kan du alltid oppdatere den.

1 Åpne ruten for beskyttelse mot phishing

Hvordan?

1. I Hjem-ruten for SecurityCenter klikker du **Internett og & nettverk.**
2. I informasjonsområdet & for Internett og nettverk klikker du**Konfigurer**.

2 I ruten for beskyttelse mot phishing, klikk på **Avansert**.

3 Under **Hviteliste,** velg det webområdet du ønsker å oppdatere, og klikk så på**Rediger.**

4 Rediger adressen til webområdet, og klikk deretter **OK**.

Fjerne et webområde fra hvitelisten

Hvis du la et webområde til hvitelisten fordi du ville ha tilgang til den, men du vil nå filtrere den, fjern den fra hvitelisten.

1 Åpne ruten for beskyttelse mot phishing

Hvordan?

1. I Hjem-ruten for SecurityCenter klikker du **Internett og & nettverk.**
2. I informasjonsområdet & for Internett og nettverk klikker du**Konfigurer**.

2 I ruten for beskyttelse mot phishing, klikk på **Avansert**.

3 Under **Hviteliste,** velg det webområdet du ønsker å fjerne, og klikk så på**Fjern.**

Deaktivere beskyttelse mot phishing

Hvis du allerede har phishingprogramvare som ikke er fra McAfee og det er en konflikt, kan du deaktivere Anti-Spam beskyttelsen mot phishing.

1 I Hjem-ruten for SecurityCenter klikker du **Internett og & nettverk.**

2 I informasjonsområdet & for Internett og nettverk klikker du**Konfigurer**.

3 Under **Phishing beskyttelse** klikker du **Av**.

Tips: Nå du er ferdig, husk å klikk på **På** under **Phishing beskyttelse** slik at du er beskyttet mot bedragerske webområder.

KAPITTEL 30

McAfee Privacy Service

Privacy Service gir avansert beskyttelse for deg, familien din, dine personlige filer og datamaskinen. Det hjelper deg med å forhindre identitetstyveri på nettet, blokkere overføring av personlig informasjon og filtrere potensielt støtende Internett-innhold (inkludert bilder). Det tilbyr også avansert foreldrestyring, som gjør at voksne kan overvåke, kontrollere og loggføre uautoriserte websøkingsvaner, og et sikkert lagringsområde for personlige passord.

Før du begynner å bruke Privacy Service, kan du gjøre deg kjent med noen av de mest populære funksjonene. Du finner mer informasjon om hvordan du konfigurerer og bruker disse funksjonene, i hjelpen for Privacy Service.

Merknad: SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer så snart det oppdager dem. Hvis du trenger hjelp til å diagnostisere beskyttelsesproblemene, kan du kjøre McAfee Virtual Technician.

I dette kapitlet

Privacy Service-funksjoner 154
Sette opp foreldrestyring 155
Beskytte opplysninger på Internett 171
Beskytte passord 173

Privacy Service-funksjoner

Privacy Service har følgende funksjoner:

- Foreldrestyring
- Beskyttelse av personlige opplysninger
- passordhvelv

Foreldrestyring

Med foreldrestyring kan du filtrere potensielt upassende bilder, konfigurere innholdsklassifiserte grupper (aldersgrupper brukes for å begrense webområder og innhold som en bruker kan vise) og angi tidsbegrensninger for bruk av Internett (tidsperioden og varigheten en bruker har tilgang til Internett) for brukere av SecurityCenter. Med foreldrestyring kan du globalt begrense brukernes tilgang til webområder samt gi og blokkere tilgang basert på aldersgrupper og tilknyttede nøkkelord.

Beskyttelse av personlige opplysninger

Beskyttelse av personlig informasjon lar deg blokkere overføringen av sensitiv eller konfidensiell informasjon (f.eks. kredittkortnummer, bankkontonummer, adresser, osv.) over Internett.

passordhvelv

Passordhvelvet er et sikkert lagringsområde for dine passord. Her kan du lagre passordene dine og være sikker på at ingen andre brukere (selv ikke en administrator) kan få tilgang til dem.

KAPITTEL 31

Sette opp foreldrestyring

Hvis dine barn bruker datamaskinen kan du konfigurere foreldrestyring for dem. Du bruker foreldrestyring til å regulere hva barn kan se og gjøre når de bruker Internett. Du kan konfigurere foreldrestyring til å aktivere eller deaktivere bildefiltrering, velge en innholdsklassifisert gruppe og angi tidsbegrensninger for bruk at Internett. Bildefiltrering blokkerer potensielt upassende bilder fra å vises når et barn søker på Internett. Den Innholdsklassifiserte gruppen angir type innhold og webområder som et barn har tilgang til, basert på barnets aldergruppe, og tidsbegrensninger for bruk av Internett angir dagene og tidspunkter et barn har tilgang til Internett. Med foreldrestyring kan du også filtrere (blokkere eller tillate) bestemte webområder for alle barn.

Merk: Du må være administrator for å sette opp foreldrestyring.

I dette kapitlet

Konfigurere brukere....156
Filtrere potensielt upassende webbilder....161
Definere innholdsklassifiseringsgruppen....162
Definere tidsbegrensninger for bruk av Internett....164
Filtrere webområder....165
Filtrere webområder med nøkkelord....168

Konfigurere brukere

Ved konfigurering av foreldrestyring, gir du tillatelser til brukere av SecurityCenter. Som standardinnstilling samsvarer SecurityCenter-brukere med Windows-brukere som er satt opp på maskinen. Hvis du imidlertid har oppgradert fra en tidligere versjon av SecurityCenter som brukte McAfee-brukere, beholdes dine McAfee-brukere og deres tillatelser.

Merknad: Du må logge det på SecurityCenter som administrator for å konfigurere brukere.

Arbeide med Windows-brukere

Du må gi tillatelser til brukere som angir hver bruker kan se og gjøre på Internett for å konfigurere foreldrekontroll. Som standardinnstilling samsvarer SecurityCenter-brukere med Windows-brukere som er satt opp på maskinen. Du legger til en bruker, redigerer kontoinformasjon for en bruker eller fjerner en bruker under Datamaskinbehandling i Windows. Du kan sette opp foreldrestyring for disse brukerne i SecurityCenter.

Hvis du oppgraderte fra en tidligere versjon av SecurityCenter som brukte McAfee-brukere, se Arbeide med McAfee-brukere (side 158).

Arbeide med McAfee-brukere

Hvis du har oppgradert fra en tidligere versjon av SecurityCenter som brukte McAfee-brukere, beholdes dine McAfee-brukere og deres tillatelser automatisk. Du kan forsette å konfigurere og administrere McAfee-brukere; men for enklere vedlikehold anbefaler McAfee at du bytter til Windows-brukere. Hvis du bytter til Windows-brukere kan du ikke bytte tilbake til McAfee-brukere.

Hvis du fortsetter å bruke McAfee-brukere, kan du legge til, redigere eller fjerne brukere og også endre eller hente administratorpassordet for McAfee.

Bytt til Windows-brukere

For enkelt vedlikehold anbefaler McAfee at du bytter til Windows-brukere. Hvis du bytter til Windows-brukere kan du ikke bytte tilbake til McAfee-brukere.

1 Åpne ruten Brukerinnstillinger

   Hvordan?

   1. Under **Vanlige oppgaver** klikker du **Hjem**.
   2. I ruten for startsiden for sikkerhetssenteret klikker du **Foreldrestyring**.
   3. I informasjonsdelen for foreldrestyring klikker du **Konfigurer**.
   4. I ruten for foreldrestyringskonfigurasjon klikker du **Avansert**.

2 Klikk på **Bytt** i ruten Brukerinnstillinger.

3 Bekreft operasjonen.

Legg til en McAfee-bruker

Etter at en McAfee-bruker er lagt til kan du konfigurere foreldrestyring for brukeren. Se Hjelp for Privacy Service for mer informasjon.

1 Logg inn på SecurityCenter som Administrator.

2 Åpne ruten Brukerinnstillinger

   Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. I ruten for startsiden for sikkerhetssenteret klikker du **Foreldrestyring**.
3. I informasjonsdelen for foreldrestyring klikker du **Konfigurer**.
4. I ruten for foreldrestyringskonfigurasjon klikker du **Avansert**.

3 Klikk på **Legg til** i ruten Brukerinnstillinger.

4 Følg instruksene på skjermen for å sette opp brukernavn, passord, kontotype og foreldrekontroll.

5 Klikk **Opprett**.

Rediger kontoinformasjon for en McAfee-bruker

Du kan endre passord, kontotype eller automatisk innloggingsmuligheter for en McAfee-bruker.

1 Logg inn på SecurityCenter som Administrator.

2 Åpne ruten Brukerinnstillinger

Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. I ruten for startsiden for sikkerhetssenteret klikker du **Foreldrestyring**.
3. I informasjonsdelen for foreldrestyring klikker du **Konfigurer**.
4. I ruten for foreldrestyringskonfigurasjon klikker du **Avansert**.

3 Klikk på et brukernavn og deretter **Rediger** i ruten Brukerinnstillinger.

4 Følg instruksene på skjermen for å redigere opp brukernavn, passord, kontotype og foreldrekontroll.

5 Klikk **OK**.

Fjern en McAfee-bruker

Du kan når som helst fjerne en McAfee-bruker.

Slik fjerner du en McAfee-bruker:

1 Logg inn på SecurityCenter som Administrator.

2 Åpne ruten Brukerinnstillinger

Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. I ruten for startsiden for sikkerhetssenteret klikker du **Foreldrestyring**.
3. I informasjonsdelen for foreldrestyring klikker du **Konfigurer**.
4. I ruten for foreldrestyringskonfigurasjon klikker du **Avansert**.

3 Velg et brukernavn og klikk deretter på **Fjern** under **McAfee-brukerkontoer** i ruten Brukerinnstillinger.

Endre administratorpassordet for McAfee

Hvis du ikke husker administratorpassordet for McAfee eller mistenker at noen kan ha fått tak i det, kan du endre det.

1 Logg inn på SecurityCenter som Administrator.

2 Åpne ruten Brukerinnstillinger

Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. I ruten for startsiden for sikkerhetssenteret klikker du **Foreldrestyring**.
3. I informasjonsdelen for foreldrestyring klikker du **Konfigurer**.
4. I ruten for foreldrestyringskonfigurasjon klikker du **Avansert**.

3 Velg **Administrator** og klikk deretter på **Fjern** under **McAfee-brukerkontoer** i ruten Brukerinnstillinger.

4 Skriv inn et nytt passord i boksen **Nytt passord** i dialogboksen Rediger brukerkonto, og skriv deretter inn passordet på nytt i boksen **Legg inn passord på nytt**.

5 Klikk **OK**.

Hente frem administratorpassordet for McAfee

Hvis du glemmer administratorpassordet, kan du hente det frem.

1 Høyreklikk på ikonet for SecurityCenter , og klikk deretter **Bytt bruker**.

2 Klikk på **Administrator** i listen **Brukernavn**, og klikk deretter på**Glemt passordet**.

3 Skriv inn svaret på ditt hemmelige spørsmål i boksen **Svar**.

4 Klikk **Send**.

Filtrere potensielt upassende webbilder

Avhengig av en brukers aldergruppe eller modenhetsnivå, kan du filtrere (blokkere eller tillate) potensielt upassende bilder når en bruker søker på Internett. Du kan for eksempel blokkere potensielt upassende bilder fra å vises når unge barn bruker Internett, men tillate dem for eldre ungdommer og voksne personer. Som standardinnstilling er bildefiltrering deaktivert for alle medlemmer i aldersgruppen Voksen. Det betyr at potensielt upassende bilder vises når disse brukerne søker på Internett. Se Definere innholdsklassifiseringsgruppen (side 162) for mer informasjon om å definere en innholdsklassifiseringsgruppe.

Filtrer potensielt upassende webbilder

Som standardinnstilling legges nye brukere til gruppen Voksen og bildefiltrering deaktiveres. Hvis du ønsker å blokkere potensielt upassende bilder fra å vises når en bestemt bruker søker på Internett, kan du aktivere bildefiltrering. Hvert potensielt upassende webbilde erstattes automatisk med et statisk McAfee-bilde.

1 Åpne ruten Brukerinnstillinger

   Hvordan?

   1. I ruten for startsiden for sikkerhetssenteret klikker du **Foreldrestyring**.
   2. I informasjonsdelen for foreldrestyring klikker du **Konfigurer**.
   3. I ruten for foreldrestyringskonfigurasjon klikker du **Avansert**.
   4. I ruten Foreldrestyring klikker du på **Brukerinnstillinger**.

2 Klikk på et brukernavn og deretter **Rediger** i ruten Brukerinnstillinger.

3 Klikk på **På** under **Bildefiltrering**, i vinduet Rediger brukerkonto.

4 Klikk **OK**.

Definere innholdsklassifiseringsgruppen

En bruker kan tilhøre følgende innholdsklassifiseringsgrupper:

- Yngre barn
- Barn
- Yngre tenåring
- Eldre tenåring
- Voksen

Privacy Service rangerer (blokkerer eller tillater) Internett-innhold basert på hvilken gruppe en bruker tilhører. Du kan dermed blokkere eller tillate visse webområder for enkelte brukere. Du kan for eksempel blokkere et webområde for brukere som ikke tilhører gruppen Yngre barn, men tillate det for brukere som tilhører gruppen Yngre tenåring. Hvis du ønsker å klassifisere innholdet for én bruker strengere enn for andre, kan du tillate denne brukeren å kun vise webområder som tillates i listen **Tillatte webområder**. Se Filtrere webområder (side 165) for mer informasjon.

Som standardinnstilling legges en ny bruker til gruppen Voksen. Det gir brukeren tilgang til alt innhold på Internett.

Definere innholdsklassifiseringsgruppe for en bruker

Som standardinnstilling legges en ny bruker til gruppen Voksen. Det gir brukeren tilgang til alt innhold på Internett. Du kan deretter justere brukerens innholdsklassifiseringsgruppe i henhold til brukerens alder og modenhetsnivå.

1 Åpne ruten Brukerinnstillinger

Hvordan?

1. I ruten for startsiden for sikkerhetssenteret klikker du **Foreldrestyring**.
2. I informasjonsdelen for foreldrestyring klikker du **Konfigurer**.
3. I ruten for foreldrestyringskonfigurasjon klikker du **Avansert**.
4. I ruten Foreldrestyring klikker du på **Brukerinnstillinger**.

2 Klikk på et brukernavn og deretter **Rediger** i ruten Brukerinnstillinger.

3 Under **Content Rating** i vinduet Rediger brukerkonto, klikker du på aldersgruppen du ønsker å tildele brukeren.

Velg avmerkingsboksen **Denne brukeren har kun tilgang til områder i listen Filtrerte webområder** for å forhindre brukeren i å søke på webområder som er blokkert i listen **Filtrerte webområder**.

4 Klikk **OK**.

Definere tidsbegrensninger for bruk av Internett

Hvis du bekymrer deg over uansvarlig eller overdreven Internett-bruk, kan du angi passende tidsbegrensninger for dine barns bruk av Internett. Når du begrenser bruken av Internett til bestemte tidspunkter for dine barn, kan du stole på at SecurityCenter vil overholde disse begrensningene - selv når du ikke er hjemme.

Som standard innstilling tillates barn å bruke Internett hele døgnet, syv dager i uken. Du kan imidlertid begrense bruken av Internett til bestemte tidspunkter eller dager, eller du kan forby bruk av Internett helt. Hvis et barn prøver å bruke Internett i en blokkert periode, varsler McAfee barnet om at det ikke er mulig. Hvis du forbyr bruk av Internett helt, kan barnet logge seg på og bruke datamaskinen, inkludert andre Internett-programmer som e-post, direktemeldinger, ftp, spill osv., men ikke søke på Internett.

Definer tidsbegrensninger for bruk av Internett

Du kan bruke rutenettet Tidsbegrensninger for bruk av Internett for å begrense et barns bruk av Internett til bestemte dager og tidspunkter.

1. Åpne ruten Brukerinnstillinger

   Hvordan?

   1. I ruten for startsiden for sikkerhetssenteret klikker du **Foreldrestyring**.
   2. I informasjonsdelen for foreldrestyring klikker du **Konfigurer**.
   3. I ruten for foreldrestyringskonfigurasjon klikker du **Avansert**.
   4. I ruten Foreldrestyring klikker du på **Brukerinnstillinger**.

2. Klikk på et brukernavn og deretter **Rediger** i ruten Brukerinnstillinger.
3. Under **Tidsbegrensninger på Internett** i vinduet Rediger brukerkonto, drar du musen for å angi dagene og tidspunktene som denne brukeren ikke kan søke på Internett.
4. Klikk **OK**.

Filtrere webområder

Du kan filtrere (blokkere eller tillate) webområder for alle brukere, unntatt dem som tilhører gruppen Voksen. Du blokkerer et webområde for å forhindre at dine barn får tilgang til det når de søker på Internett. Hvis et barn prøver å få tilgang til et blokkert webområde, vises en melding om at området ikke er tilgjengelig fordi det er blokkert av McAfee.

Hvis McAfee har som standardinnstilling har blokkert et webområde du ønsker at dine barn skal ha tilgang til, kan du tillate dette webområdet. Se Filtrere webområder med nøkkelord (side 168) for mer informasjon om webområder som blokkeres automatisk av McAfee. Du kan også når som helst oppdatere eller fjerne et webområde.

Merknad: Brukere (inkludert administratorer) som tilhører gruppen Voksen har tilgang til alle webområder, inkludert de som er blokkert. Du må logge deg på som en ikke-voksen bruker for å teste de blokkerte webområdene.

Blokkere et webområde

Du blokkerer et webområde for å forhindre at dine barn får tilgang til det når de søker på Internett. Hvis et barn prøver å få tilgang til et blokkert webområde, vises en melding som indikerer at området ikke er tilgjengelig fordi det er blokkert av McAfee.

1 Åpne ruten Foreldrestyring.

   Hvordan?

   1. I ruten for startsiden for sikkerhetssenteret klikker du **Foreldrestyring**.
   2. I informasjonsdelen for foreldrestyring klikker du **Konfigurer**.
   3. I ruten for foreldrestyringskonfigurasjon må du kontrollere at foreldrestyring er aktivert. Deretter klikker du **Avansert**.

2 I ruten foreldrestyring klikker du **Filtrerte webområder**.

3 I ruten Filtrerte webområder skriver du inn en webadresse i boksen **http://**, og klikker deretter på **Blokker**.

4 Klikk **OK**.

Tips: Du kan blokkere et webområde som tidligere er tillatt ved å klikke på adressen til webområdet i listen **Filtrerte webområder**, og deretter klikke på **Blokker**.

Tillat et webområde

Du tillater et webområde for å sikre at det ikke er blokkert for noen brukere. Hvis du tillater et webområde som McAfee som standard har blokkert, overstyrer du standardinnstillingen.

1 Åpne ruten Foreldrestyring.

   Hvordan?

   1. I ruten for startsiden for sikkerhetssenteret klikker du **Foreldrestyring**.
   2. I informasjonsdelen for foreldrestyring klikker du **Konfigurer**.
   3. I ruten for foreldrestyringskonfigurasjon må du kontrollere at foreldrestyring er aktivert. Deretter klikker du **Avansert**.

2 I ruten foreldrestyring klikker du **Filtrerte webområder**.

3 I ruten Filtrerte webområder skriver du inn en webadresse i boksen **http://**, og klikker deretter på **Tillat**.

4 Klikk **OK**.

Tips: Du kan tillate et webområde som tidligere er blokkert ved å klikke på adressen til webområdet i listen **Filtrerte webområder**, og deretter klikke på **Tillat**.

Oppdatere et filtrert webområde

Hvis adressen for et webområde endres, eller du legger inn feil adresse når du blokkerer eller tillater området, kan du oppdatere den.

1 Åpne ruten Foreldrestyring.

   Hvordan?

   1. I ruten for startsiden for sikkerhetssenteret klikker du **Foreldrestyring**.
   2. I informasjonsdelen for foreldrestyring klikker du **Konfigurer**.
   3. I ruten for foreldrestyringskonfigurasjon må du kontrollere at foreldrestyring er aktivert. Deretter klikker du **Avansert**.

2 I ruten Foreldrestyring klikker du **Filtrerte webområder**.

3 I ruten Filtrerte webområder klikker på du en oppføring i listen **Filtrerte webområder**, endrer webadressen i boksen**http://** og klikker på **Oppdater**.

4 Klikk **OK**.

Fjerne et filtrert webområde

Du kan fjerne et filtrert webområde hvis du ikke lenger ønsker å blokkere eller tillate det.

1 Åpne ruten Foreldrestyring.

Hvordan?

1. I ruten for startsiden for sikkerhetssenteret klikker du **Foreldrestyring**.
2. I informasjonsdelen for foreldrestyring klikker du **Konfigurer**.
3. I ruten for foreldrestyringskonfigurasjon må du kontrollere at foreldrestyring er aktivert. Deretter klikker du **Avansert**.

2 I ruten Foreldrestyring klikker du **Filtrerte webområder**.

3 I ruten Filtrerte webområder klikker du en oppføring i listen **Filtrerte webområder**, og klikker deretter på **Fjern**.

4 Klikk **OK**.

Filtrere webområder med nøkkelord

Med nøkkelordfiltrering kan du blokkere brukere som ikke er voksne fra å besøke webområder som inneholder potensielt upassende tekst. Når nøkkelordfiltrering er aktivert brukes en standardliste over nøkkelord og tilsvarende regler til å rangere innhold i samsvar med deres innholdsklassifiseringsgruppe. Brukere må tilhøre en bestemt gruppe for å få tilgang til webområder som inneholder bestemte nøkkelord. Kun medlemmer av gruppen Voksen kan for eksempel besøke webområder som inneholder ordet *porno*, og kun medlemmer fra gruppen Barn (og eldre) kan besøke webområder som inneholder ordet *narkotika*.

Du kan også legge til dine egne nøkkelord i standardlisten, og knytte disse til bestemte innholdsklassifiseringsgrupper. Nøkkelordregler som du legger til, overstyrer regler som allerede er knyttet til nøkkelord som stemmer overens med nøkkelord i standardlisten.

Deaktivere nøkkelordfiltrering

Som standardinnstilling er nøkkelordfiltrering aktivert. Det betyr at en standardliste over nøkkelord og tilsvarende regler brukes til å rangere innhold i samsvar med deres innholdsklassifiseringsgruppe. Selv om McAfee ikke anbefaler det, kan du deaktivere nøkkelordfiltrering når som helst.

1 Åpne ruten Foreldrestyring.

Hvordan?

1. I ruten for startsiden for sikkerhetssenteret klikker du **Foreldrestyring**.
2. I informasjonsdelen for foreldrestyring klikker du **Konfigurer**.
3. I ruten for foreldrestyringskonfigurasjon må du kontrollere at foreldrestyring er aktivert. Deretter klikker du **Avansert**.

2 I ruten Foreldrestyring klikker du på **Nøkkelord**.

3 I ruten Nøkkelord klikker du **Av**.

4 Klikk **OK**.

Blokkere webområder basert på nøkkelord

Hvis du vil blokkere webområder på grunn av upassende innhold, men ikke vet hva de bestemte webadressene er, kan du blokkere webområder basert på deres nøkkelord. Angi et nøkkelord og bestem hvilke innholdsklassifiseringsgrupper som skal ha tilgang til webområder som inneholder det bestemte nøkkelordet.

1 Åpne ruten Foreldrestyring.

Hvordan?

1. I ruten for startsiden for sikkerhetssenteret klikker du **Foreldrestyring**.
2. I informasjonsdelen for foreldrestyring klikker du **Konfigurer**.
3. I ruten for foreldrestyringskonfigurasjon må du kontrollere at foreldrestyring er aktivert. Deretter klikker du **Avansert**.

2 Klikk på **Nøkkelord** i ruten Foreldrestyring og kontroller at nøkkelordfiltrering er aktivert.

3 Skriv inn et nøkkelord i boksen **Se etter** under **Nøkkelordliste**.

4 Flytt glidebryteren **Minstealder** for å angi minstealder for en aldersgruppe.
Brukere i denne alderen og eldre kan besøke webområder som inneholder nøkkelordet.

5 Klikk **OK**.

KAPITTEL 32

Beskytte opplysninger på Internett

Ved å blokkere informasjon kan du beskytte privat informasjon og filer når du søker på Internett. Du kan for eksempel forhindre at personlige opplysninger (for eksempel navn, adresse, kredittkort- og bankkontonumre) overføres via Internett ved å legge dem til området for blokkert informasjon.

Merknad: Privacy Service blokkerer ikke overføring av personlig informasjon sikre webområder (Dvs. webområder som bruker protokollen https://), som for eksempel Nettbanksider.

I dette kapitlet

Beskytte personlige opplysninger 172

Beskytte personlige opplysninger

Forhindre at personlige opplysninger (for eksempel navn, adresse, kredittkort- og bankkontonumre) overføres via Internett ved å blokkert informasjonen. Hvis McAfee oppdager at personlig informasjon (i for eksempel et skjema eller fil) holder på å bli sendt over Internett vil følgende skje:

- Hvis du er administrator, må du bekrefte om opplysningene skal sendes eller ikke.
- Hvis du ikke er administrator, erstattes den blokkerte delen med stjerner (*). Hvis for eksempel et ondsinnet webområde forsøker å sende ditt kredittkortnummer til en annen maskin, vil nummeret erstattes med stjerner.

Beskytt personlige opplysninger

Du kan blokkere følgende typer personlige opplysninger: navn, adresse, postnummer, personnummer, telefonnummer, kredittkortnumre, bankkontoer, aksjekontoer og telefonkort. Hvis du vil blokkere andre typer personlige opplysninger, kan du angi typen til **annet**.

1. Åpne ruten Beskyttet informasjon.

   Hvordan?

   1. Under **Vanlige oppgaver** klikker du **Hjem**.
   2. I Hjem-ruten for SecurityCenter klikker du **Internett og& nettverk**.
   3. I informasjonsdelen for Internett og nettverk klikker du **Konfigurer**.
   4. Kontroller at beskyttelse av personlige opplysninger er aktivert i ruten for Internett-konfigurasjon, og klikk deretter **Avansert**.

2. I ruten Beskyttet informasjon klikker du på **Legg til**.
3. Velg typen opplysninger du vil blokkere, fra listen.
4. Oppgi dine personlige opplysninger og klikk deretter **OK**.

KAPITTEL 33

Beskytte passord

Passordhvelvet er et sikkert lagringsområde for dine passord. Her kan du lagre passordene dine og være sikker på at ingen andre brukere (selv ikke en administrator) kan få tilgang til dem.

I dette kapitlet

Konfigurere passordhvelvet 174

Konfigurere passordhvelvet

Før du kan bruke passordhvelvet, må du angi et passord for passordhvelvet. Bare brukere som kjenner dette passordet har tilgang til ditt passordhvelv. Hvis du glemmer passordet for passordhvelvet, kan du tilbakestille det. Alle passordene som var lagret i passordhvelvet, blir imidlertid slettet.

Etter at du har angitt et passord for passordhvelvet, kan du legge til, endre eller fjerne passord fra hvelvet. Du kan også når som helst endre passordet for passordhvelvet.

Legge til et passord

Hvis du har problemer med å huske passordene dine, kan du legge dem til i passordhvelvet. Passordhvelvet er et sikkert sted som bare brukere som kjenner til passordet for passordhvelvet, har tilgang til.

1 Åpne ruten Passordhvelv.

Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. I Hjem-ruten for SecurityCenter klikker du **Internett og& nettverk**.
3. I informasjonsdelen for Internett og nettverk klikker du **Konfigurer**.
4. I ruten for Internett- og nettverkskonfigurasjon klikker du **Avansert** under **Passordhvelv**.

2 Skriv inn passordet for passordhvelvet i boksen **Passord**, og skriv det inn på nytt i boksen **Legg inn passord på nytt**.

3 Klikk **Åpne**.

4 Klikk på **Legg til** i ruten Administrer passordhvelv.

5 Skriv inn en beskrivelse av passordet (for eksempel hva det er til) i **Beskrivelse**-boksen, og skriv det inn i **Passord**-boksen.

6 Klikk **OK**.

Endre et passord

For å sikre at oppføringene i passordhvelvet er nøyaktige og pålitelige, må du oppdatere dem hvis passordene blir endret.

1 Åpne ruten Passordhvelv.

Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. I Hjem-ruten for SecurityCenter klikker du **Internett og& nettverk**.
3. I informasjonsdelen for Internett og nettverk klikker du **Konfigurer**.
4. I ruten for Internett- og nettverkskonfigurasjon klikker du **Avansert** under **Passordhvelv**.

2 Skriv inn passordet for passordhvelvet i **Passord**-boksen.

3 Klikk **Åpne**.

4 I ruten Administrere passordhvelv klikker du en passordoppføring. Klikk deretter **Rediger**.

5 Endre beskrivelsen av passordet (for eksempel hva det er til) i **Beskrivelse**-boksen, eller endre passordet i **Passord**-boksen.

6 Klikk **OK**.

Fjerne et passord

Du kan fjerne et passord fra passordhvelvet når som helst. Det går ikke an å gjenopprette et passord som fjernes fra hvelvet.

1 Åpne ruten Passordhvelv.

Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. I Hjem-ruten for SecurityCenter klikker du **Internett og& nettverk**.
3. I informasjonsdelen for Internett og nettverk klikker du **Konfigurer**.
4. I ruten for Internett- og nettverkskonfigurasjon klikker du **Avansert** under **Passordhvelv**.

2 Skriv inn passordet for passordhvelvet i **Passord**-boksen.

3 Klikk **Åpne**.

4 I ruten Administrer passordhvelv klikker du en passordoppføring. Klikk deretter **Fjern**.

5 I bekreftelsesdialogboksen for fjerning klikker du **Ja**.

Endre passord for passordhvelv

Du kan når som helst endre passordet for passordhvelvet.

1 Åpne ruten Passordhvelv.

Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. I Hjem-ruten for SecurityCenter klikker du **Internett og& nettverk**.
3. I informasjonsdelen for Internett og nettverk klikker du **Konfigurer**.
4. I ruten for Internett- og nettverkskonfigurasjon klikker du **Avansert** under **Passordhvelv**.

2 Skriv inn ditt nåværende passord i boksen **Passord** i ruten Passordhvelv, og klikk deretter på **Åpne**.

3 Klikk på **Endre passord** i ruten Administrer passordhvelv.

4 Skriv et nytt passord i boksen **Velg passord**, og skriv det inn på nytt i boksen **Legg inn passord på nytt**.

5 Klikk **OK**.

6 Klikk på **OK** i dialogboksen Passord endret for passordhvelv.

Tilbakestille passord for passordhvelv

Hvis du glemmer passordet for passordhvelvet, kan du tilbakestille det. Alle passordene som du tidligere har angitt, blir imidlertid slettet.

1 Åpne ruten Passordhvelv.

Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. I Hjem-ruten for SecurityCenter klikker du **Internett og& nettverk**.
3. I informasjonsdelen for Internett og nettverk klikker du **Konfigurer**.
4. I ruten for Internett- og nettverkskonfigurasjon klikker du **Avansert** under **Passordhvelv**.

2 Under **Tilbakestill passordhvelv** skriver du inn et nytt passord i **Passord**-boksen. Deretter skriver du det inn på nytt i boksen **Skriv inn passord på nytt**.

3 Klikk **Tilbakestill**.

4 I dialogboksen for bekreftelse av tilbakestilling av passord, klikker du **Ja**.

KAPITTEL 34

McAfee Data Backup

Du kan bruke Data Backup til å unngå tap av data ved å arkivere filer til CD, DVD, USB-stasjon, ekstern harddisk eller nettverksstasjon. Med lokal arkivering kan du arkivere (sikkerhetskopiere) personlig data til CD, DVD, USB-stasjon, ekstern harddisk eller nettverksstasjon. Dermed får du en lokal kopi av dataene, dokumentene og andre personlige ting i tilfelle de ved et uhell skulle gå tapt.

Før du begynner å bruke Data Backup, kan du gjøre deg kjent med noen av de mest populære funksjonene. Data Backup-hjelp har informasjon om å konfigurere og bruke disse funksjonene. Når du har sett gjennom programfunksjonene, må du passe på at du har nok tilgjengelig arkiveringsmedia til å utføre lokal arkivering.

I dette kapitlet

Funksjoner 178
Arkivere filer 179
Arbeide med arkiverte filer 187

Funksjoner

Data Backup har følgende funksjoner for å lagre og gjenopprette bilder, musikk og andre viktige filer.

Planlagt lokal arkivering

Beskytt din data ved å arkivere filer og mapper til CD, DVD, USB-stasjon, ekstern harddisk eller nettverksstasjon. Etter den første arkiveringen, skjer trinnvise arkiveringer automatisk.

Ett-klikks-gjenoppretting

Hvis filer og mapper på din datamaskin slettes ved et uhell eller blir skadet, kan du hente den siste arkiverte versjonen fra aktuelt arkivert media.

Komprimering og kryptering

De arkiverte filene komprimeres automatisk, noe som sparer plass i arkivmedia. Arkivene dine krypteres som standard, som et ekstra sikkerhetstiltak.

KAPITTEL 35

Arkivere filer

Du kan bruke McAfee Data Backup til å arkivere kopier av filene til CD, DVD, USB-stasjon, ekstern harddisk eller nettverksstasjon. Hvis du arkiverer filene dine på denne måten, kan du enkelt hente informasjon hvis noe går tapt eller ødelegges ved et uhell.

Før du begynner å arkivere filer, må du velge arkivplassering (CD, DVD, USB-stasjon, ekstern harddisk eller nettverksstasjon). McAfee har forhåndsinnstilt noen andre innstillinger, som for eksempel hvilke mapper og filtyper du vil arkivere, men du kan endre disse innstillingene.

Når du har stilt inn de lokale arkiveringsalternativene, kan du endre standardinnstilling for hvor ofte Data Backup kjører fullstendig arkivering eller hurtigarkivering. Du kan når som helst kjøre manuell arkivering.

I dette kapitlet

Stille inn arkiveringsalternativer 180
Kjøre fullstendig arkivering og hurtigarkivering 184

Stille inn arkiveringsalternativer

Før du begynner å arkivere data, må du stille inn noen arkiveringsalternativer. Du må for eksempel velge oppsiktsplassering og oppsiktsfiltyper. Oppsiktsplassering er mapper på datamaskinen din som Data Backup overvåker for å finne nye filer eller filendringer. Oppsiktsfiltyper er alle typer filer (for eksempel .doc, og .xls) som Data Backup arkiverer i oppsiktsplasseringene. Data Backup holder som standard oppsikt med alle filtyper i oppsiktsplasseringene.

Du kan velge to typer oppsiktsplasseringer: omfattende oppsiktsplasseringer og overfladiske oppsiktsplasseringer. Hvis du oppretter en omfattende oppsiktsplassering, tas oppsiktsfilene i den mappen og undermappene med i arkiveringen. Hvis du oppretter en overfladisk oppsiktsplassering, tas kun oppsiktsfilene i den mappen (ikke undermappene) med i arkiveringen. Du kan også identifisere plasseringer som du ikke vil ta med i arkiveringen. Windows Skrivebord og Mine dokumenter er som standard valgt som omfattende oppsiktsplasseringer.

Når du har stilt inn oppsiktsfiltyper og -plassering, må du velge arkivplassering (dvs. CD, DVD, USB-stasjon, ekstern harddisk eller nettverksstasjon der den arkiverte dataen skal lagres). Du kan når som helst endre arkivplasseringen.

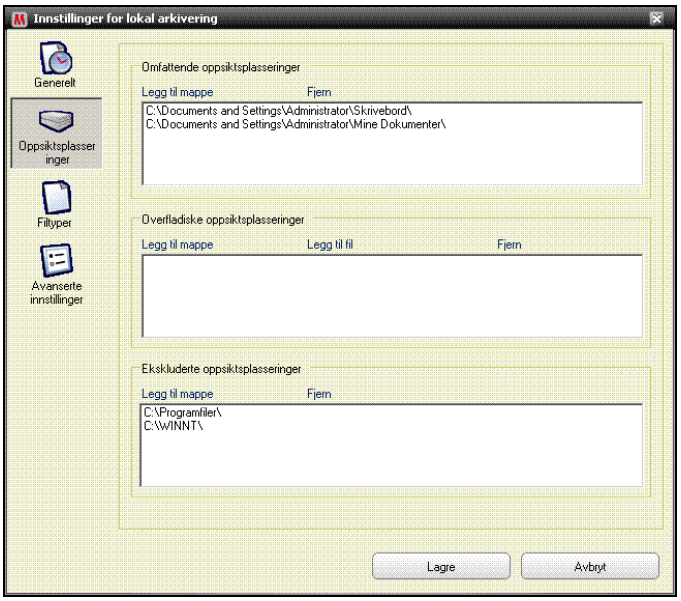
Av sikkerhetshensyn eller størrelseshensyn, krypteres eller komprimeres de arkiverte filene som standard. Innholdet i de krypterte filene omformes fra tekst til kode, og informasjonen skjules slik at den ikke kan leses av folk som ikke vet hvordan de skal dekryptere den. Komprimerte filer er komprimert til en form som minimerer plassen som kreves for lagring eller overføring. Selv om McAfee ikke anbefaler det, kan du når som helst deaktivere kryptering eller komprimering.

Ta med en plassering i arkivet

Du kan velge to typer oppsiktsplasseringer for arkivering: omfattende eller overfladisk. Hvis du oppretter en omfattende oppsiktsplassering, overvåker Data Backup innholdet i mappen og undermappene og ser etter endringer. Hvis du oppretter en overfladisk oppsiktsplassering, overvåker Data Backup kun innholdet i mappen (ikke undermappene).

Slik tar du med en plassering i arkivet:

1. Klikk på kategorien **Lokal arkivering**.
2. Klikk på **Innstillinger** i venstre rute.
3. I dialogboksen Innstillinger for lokal arkivering klikker du på **Oppsiktsplasseringer**.



4. Gjør ett av følgende:
   - Hvis du vil arkivere innholdet i en mappe og dens undermapper, klikker du på **Legg til mappe** under **Omfattende oppsiktsplasseringer**.
   - Hvis du vil arkivere innholdet i en mappe, men ikke dens undermapper, klikker du på **Legg til mappe** under **Overfladiske oppsiktsplasseringer**.
5. I Finn mappe-dialogboksen navigerer du til mappen du vil overvåke og klikker på **OK**.
6. Klikk på **Lagre**.

Tips: Hvis du vil at Data Backup skal overvåke en mappe som du ikke har opprettet ennå, kan du klikke på **Opprett ny mappe** i Finn mappe-dialogboksen for å legge til en mappe og stille inn oppsiktsplasseringen samtidig.

Stille inn filtyper for arkivering

Du kan spesifisere hvilke filtyper som skal arkiveres i dine omfattende eller overfladiske oppsiktsplasseringer. Du kan velge fra en eksisterende liste over filtyper eller legge til nye typer i listen.

Slik stiller du inn filtyper for arkivering:

1. Klikk på kategorien **Lokal arkivering**.
2. Klikk på **Innstillinger** i venstre rute.
3. I dialogboksen Innstillinger for lokal arkivering klikker du på **Filtyper**.
4. Utvid listen over filtyper og merk av i boksene ved siden av filtypene du vil arkivere.
5. Klikk på **Lagre**.

Tips: Hvis du vil legge til en ny filtype i listen **Valgte filtyper**, skriv inn filtype i boksen **Legg til tilpasset filtype i "Annet"** og klikk på **Legg til**. Den nye filtypen blir automatisk en oppsiktsfil.

Utelate en plassering fra arkivet

Du kan utelate en plassering fra arkivet hvis du vil forhindre at plasseringen (mappen) og innholdet skal bli arkivert.

Slik utelater du en plassering fra arkivet:

1. Klikk på kategorien **Lokal arkivering**.
2. Klikk på **Innstillinger** i venstre rute.
3. I dialogboksen Innstillinger for lokal arkivering klikker du på **Oppsiktsmapper**.
4. Klikk på **Legg til mappe** under **Ekskluderte oppsiktsplasseringer**.
5. I Finn mappe-dialogboksen navigerer du til mappen du vil ekskludere, velger den og klikker på **OK**.
6. Klikk på **Lagre**.

Tips: Hvis du vil at Data Backup skal ekskludere en mappe som du ikke har opprettet ennå, kan du klikke på **Opprette ny mappe** i Finn mappe-dialogboksen for å legge til en mappe og samtidig ekskludere den.

Endre arkivplasseringen

Når du endrer arkivplassering, vises filer som tidligere var arkivert andre steder, som *Aldri arkivert*.

Slik endrer du arkivplasseringen:

1. Klikk på kategorien **Lokal arkivering**.
2. Klikk på **Innstillinger** i venstre rute.
3. Klikk på **Endre arkivplassering**.
4. Gjør ett av følgende i Arkivplassering-dialogboksen:
   - Klikk på **Velg CD / DVD-brenner**, klikk på datamaskinens CD- eller DVD-stasjon i listen **Brenner** og klikk deretter på **Lagre**.
   - Klikk på **Velg stasjonsplassering**, gå til en USB-stasjon, lokalstasjon eller ekstern harddisk, velg den og klikk så på **OK**.
   - Klikk på **Velg nettverksplassering**, gå til en nettverksmappe, velg den og klikk så på **OK**.
5. Godkjenn den nye arkivplasseringen i **Valgt arkivplassering** og klikk deretter på **OK**.
6. Klikk på **OK** i bekreftelsesdialogboksen.
7. Klikk på **Lagre**.

Deaktivere arkiveringskryptering og -komprimering

Kyptering av arkiverte filer beskytter dataen din ved å skjule innholdet i filene slik at de er uleselige. Komprimering av arkiverte filer minimerer filstørrelsen. Både kryptering og komprimering er aktivert som standard, men du kan når som helst deaktivere dem.

Slik deaktiverer du arkiveringskryptering og -komprimering:

1. Klikk på kategorien **Lokal arkivering**.
2. Klikk på **Innstillinger** i venstre rute.
3. I dialogboksen Innstillinger for lokal arkivering klikker du på **Avanserte innstillinger**.
4. Tøm boksen **Aktiver kryptering for å øke sikkerheten**.
5. Tøm boksen **Aktiver komprimering for å redusere lagring**.
6. Klikk på **Lagre**.

Merk: McAfee anbefaler at du ikke deaktiverer kryptering og komprimering når du arkiverer filer.

Kjøre fullstendig arkivering og hurtigarkivering

Du kan velge to typer arkivering: fullstendig eller hurtig. Når du kjører fullstendig arkivering, arkiverer du et fullstendig datasett basert på oppsiktsfilene og plasseringene du har konfigurert. Når du kjører hurtigarkivering, arkiverer du kun oppsiktsfilene som har endret seg siden forrige fullstendige arkivering eller hurtigarkivering.

Data Backup kjører som standard en fullstendig arkivering av oppsiktsfilene i oppsiktsplasseringene hver mandag kl. 09.00, og en hurtigarkivering hver 48. time etter siste fullstendige arkivering eller hurtigarkivering. Denne tidsplanen sørger for at du alltid har et oppdatert arkiv av filene dine. Hvis du ikke vil arkivere hver 48. time, kan du imidlertid justere tidsplanen etter behov.

Du kan arkivere innholdet i oppsiktsplasseringene når du vil. Hvis du endrer en fil og vil arkivere den, men Data Backup ikke skal kjøre en fullstendig arkivering eller hurtigarkivering før om noen timer, kan du arkivere filene manuelt. Når du arkiverer filene manuelt, tilbakestilles intervallet for automatisk arkivering.

Du kan også avbryte en automatisk eller manuell arkivering hvis den kjøres på et upassende tidspunkt. Hvis du for eksempel utfører en ressurskrevende oppgave og den automatiske arkiveringen starter, kan du stanse den. Når du stanser en automatisk arkivering, tilbakestilles intervallet for automatisk arkivering.

Planlegge automatiske arkiveringer

Du kan velge hvor ofte fullstendig arkivering og hurtigarkivering kjøres for å sikre at dataene dine alltid er beskyttet.

Slik planlegger du automatiske arkiveringer:

1. Klikk på kategorien **Lokal arkivering**.
2. Klikk på **Innstillinger** i venstre rute.
3. I dialogboksen Innstillinger for lokal arkivering klikker du på **Generelt**.
4. Hvis du vil kjøre en fullstendig arkivering hver dag, uke eller måned, klikker du ett av følgende under **Fullstendig arkivering hver**:
   - **Dag**
   - **Uke**
   - **Måned**

5 Merk av i boksene ved siden av dagen du vil kjøre fullstendig arkivering.

6 Klikk på en verdi i listen **Ved** for å spesifisere når du vil kjøre fullstendig arkivering.

7 Hvis du vil kjøre en hurtigarkivering hver time, klikker du på ett av følgende under **Hurtigarkivering**:

- **Timer**
- **Dager**

8 Skriv inn et tall som representerer hvor ofte i boksen **Hurtigarkivering hver**.

9 Klikk på **Lagre**.

Avbryte en automatisk arkivering

Data Backup kjører en automatisk arkivering av filer i oppsiktsplasseringer i henhold til tidsplanen du har definert. Du kan imidlertid avbryte en automatisk arkivering mens den holder på.

Slik avbryter du en automatisk arkivering:

1 Klikk på **Stopp arkivering** i venstre rute.

2 Klikk på **Ja** i bekreftelsesdialogboksen.

Merk: Koblingen **Stopp arkivering** vises kun når en sikkerhetskopiering pågår.

Kjøre manuell arkivering

Automatisk arkivering kjøres i henhold til en forhåndsdefinert tidsplan. Du kan kjøre en manuell hurtigarkivering eller fullstendig arkivering når som helst. Hurtigarkivering arkiverer kun filene som har endret seg siden forrige fullstendige arkivering eller hurtigarkivering. En fullstendig arkivering arkiverer oppsiktsfiler i alle oppsiktsplasseringer.

Slik kjører du en manuell hurtigarkivering eller fullstendig arkivering:

1 Klikk på kategorien **Lokal arkivering**.

2 Hvis du vil kjøre en hurtigarkivering, klikker du på **Hurtigarkivering** i venstre rute.

3 Hvis du vil kjøre en fullstendig arkivering, klikker du på **Fullstendig arkivering** i venstre rute.

4 I dialogboksen Klar til å starte arkivering bekrefter du lagringsplass og innstillinger, og klikker deretter på **Fortsett**.

KAPITTEL 36

Arbeide med arkiverte filer

Når du har arkivert noen filer, kan du bruke Data Backup til å jobbe med dem. De arkiverte filene vises i et vanlig utforskervindu slik at du lett kan finne dem. Etter hvert som arkivet vokser, vil du kanskje sortere filene eller lete etter dem. Du kan også åpne filene direkte i utforskervinduet for å undersøke innholdet uten å hente filene.

Du henter filer fra et arkiv hvis den lokale filkopien er utdatert, blir skadet eller hvis den mangler. Data Backup gir deg den informasjonen du trenger for å håndtere de lokale arkivene og lagringsmedia.

I dette kapitlet

Bruke utforskeren for lokal arkivering 188
Gjenopprette arkiverte filer 190
Håndtere arkiver 192

Bruke utforskeren for lokal arkivering

Med utforskeren for lokal arkivering kan du se og endre filene du har arkivert lokalt. Du kan se hver fils navn, type, plassering, størrelse, status (dvs. arkivert, ikke arkivert eller arkivering pågår) samt datoen hver fil sist ble arkivert. Du kan også sortere filene etter disse kriteriene.

Hvis du har et stort arkiv, kan du enkelt finne en fil ved å søke etter den. Du kan søke etter hele eller deler av filnavnet eller -banen, og du kan begrense søket ved å spesifisere omtrentlig filstørrelse og datoen for siste arkivering.

Etter at du har funnet en fil, kan du åpne den direkte i utforsker for lokal arkivering. Data Backup åpner filen i standardprogrammet slik at du kan foreta endringer uten å forlate utforskeren. Filen lagres til den originale oppsiktsplasseringen på datamaskinen din, og arkiveres automatisk i henhold til tidsplanen.

Sortere arkiverte filer

Du kan sortere de arkiverte filene og mappene etter følgende kriterier: navn, filtype, størrelse, status (dvs. arkivert, ikke arkivert eller arkivering pågår) samt datoen filene sist ble arkivert.

Slik sorterer du arkiverte filer:

1. Klikk på kategorien **Lokal arkivering**.
2. Klikk på et kolonnenavn i den høyre ruten.

Søke etter en arkivert fil

Hvis du har en stor database med arkiverte filer, kan du enkelt finne en fil ved å søke etter den. Du kan søke etter hele eller deler av filnavnet eller -banen, og du kan begrense søket ved å spesifisere omtrentlig filstørrelse og datoen for siste arkivering.

Slik søker du etter en arkivert fil:

1. Skriv inn hele eller deler av filnavnet i **Søk**-boksen øverst i skjermbildet og trykk deretter på ENTER.
2. Skriv inn hele eller deler av banen i boksen **Hele eller del av banen**.
3. Spesifiser omtrentlig størrelse på filen du leter etter ved å gjøre ett av følgende:
   - Klikk på **<100 kB**, **<1 MB**, eller **>1 MB**.
   - Klikk på **Størrelse i kB** og spesifiser omtrentligr størrelsesverdier i boksene.
4. Spesifiser omtrentlig størrelse på filens siste sikkerhetskopiering ved å gjøre ett av følgende:
   - Klikk på **Denne uke**, **Denne måned** eller **Dette år**.

- Klikk på **Angi datoer**, klikk på **Arkivert** i listen, og klikk deretter på den passende verdien fra datolisten.

5 Klikk på **Søk**.

Merk: Hvis du ikke vet omtrentlig størrelse eller dato for siste sikkerhetskopiering, klikker du på **Ukjent**.

Åpne en arkivert fil

Du kan undersøke innholdet til en arkivert fil ved å åpne den direkte i utforskeren for lokal arkivering.

Slik åpner du arkiverte filer:

1 Klikk på kategorien **Lokal arkivering**.

2 Klikk filnavnet i den høyre ruten og klikk deretter på **Åpne**.

Tips: Du kan også åpne en arkivert fil ved å dobbeltklikke på filnavnet.

Gjenopprette arkiverte filer

Hvis en oppsiktsfil blir skadet, forsvinner eller slettes ved et uhell, kan du hente en kopi fra et lokalt arkiv. Derfor er det viktig at du arkiverer filene dine med jevne mellomrom. Du kan også gjenopprette eldre versjoner av filer fra et lokalt arkiv. Hvis du for eksempel arkiverer en fil regelmessig, men vil gå tilbake til en tidligere filversjon, kan du gjøre det ved å finne filen i arkivplasseringen. Hvis arkivplasseringen er en lokal stasjon eller nettverksstasjon, kan du lete etter filen. Hvis arkivplasseringen er en ekstern harddisk eller USB-stasjon, må du koble den aktuelle enheten til datamaskinen og deretter lete etter filen. Hvis arkivplasseringen er en CD eller DVD, må du sette CD-en eller DVD-en i datamaskinen og deretter lete etter filen.

Du kan også gjenopprette filer som du har arkivert på en datamaskin, fra en annen datamaskin. Hvis du for eksempel arkiverer noen filer til en ekstern harddisk på datamaskin A, kan du gjenopprette dem på datamaskin B. Du må installere McAfee Data Backup på datamaskin B og koble til den eksterne harddisken for å få dette til. Deretter må du finne filene i Data Backup, og de legges til i listen **Manglende filer** slik at de kan gjenopprettes.

Hvis du vil ha mer informasjon om å arkivere filer, kan du lese Arkivere filer. Hvis du sletter en oppsiktsfil fra datamaskinen med vilje, kan du også slette oppføringen fra listen **Manglende filer**.

Gjenopprette manglende filer fra et lokalt arkiv

Med Data Backups lokale arkiv kan du også gjenopprette data som mangler fra en oppsiktsmappe på din lokale datamaskin. Hvis en fil for eksempel flyttes ut av en oppsiktsmappe eller slettes, og den allerede er arkivert, kan du gjenopprette den fra det lokale arkivet.

Slik henter du en manglende fil fra et lokalt arkiv:

1. Klikk på kategorien **Lokal arkivering**.
2. I kategorien **Manglende filer** nederst på skjermen merker du av i boksen ved siden av navnet på filen du vil gjenopprette.
3. Klikk på **Gjenopprett**.

Tips: Du kan gjenopprette alle filene i listen **Manglende filer** ved å klikke på **Gjenopprett alle**.

Gjenopprette en eldre filversjon fra et lokalt arkiv

Hvis du vil gjenopprette en eldre versjon av en arkivert fil, kan du finne den og legge den til i listen **Manglende filer**. Deretter kan du gjenopprette filen, som du ville gjort med en hvilken som helst fil i listen **Manglende filer**.

Slik gjenoppretter du en eldre filversjon fra et lokalt arkiv:

1. Klikk på kategorien **Lokal arkivering**.
2. I kategorien **Manglende filer** nederst på skjermen klikker du på **Bla gjennom** og navigerer til stedet der arkivet er lagret.

   Navnene på arkiverte mapper har følgende format: `opr ddmmåå_tt-mm-ss_***`, der `ddmmåå` er datoen filene ble arkivert, `tt-mm-ss` er tidspunktet filene ble arkivert, og `***` er enten `Full` eller `Inc`, alt ettersom det var en fullstendig arkivering eller en hurtigarkivering.
3. Velg plassering og klikk deretter på **OK**.

   Filene i valgt plassering vises i listen **Manglende filer** og er klare til å gjenopprettes. Du finner mer informasjon i Gjenopprette manglende filer fra et lokalt arkiv.

Fjerne filer fra listen over manglende filer

Når en arkivert fil flyttes ut av en oppsiktsmappe eller slettes, vises den automatisk i listen **Manglende filer**. Dermed kan du se at det er en uregelmessighet mellom de arkiverte filene på nettet og filene i oppsiktsmappene. Hvis filen ble flyttet ut av oppsiktsmappen eller slettet med vilje, kan du slette filen fra listen **Manglende filer**.

Slik fjerner du en fil fra listen over manglende filer:

1. Klikk på kategorien **Lokal arkivering**.
2. I kategorien **Manglende filer** nederst på skjermen merker du av i boksen ved siden av navnet på filen du vil fjerne.
3. Klikk på **Slett**.

Tips: Du kan fjerne alle filene i listen **Manglende filer** ved å klikke på **Slett alle**.

Håndtere arkiver

Du kan se et sammendrag av informasjonen om fullstendig arkivering og hurtigarkivering når som helst. Du kan for eksempel se informasjon om hvor mye data som holdes under oppsikt, hvor mye data som er arkivert, og hvor mye data som er under oppsikt, men som ikke er arkivert ennå. Du kan også se informasjon om arkiveringstidplanen din, som dato for nyeste eller neste arkivering.

Vise et sammendrag av arkiveringssaktiviteten

Du kan vise informasjonen om arkiveringsaktiviteten når som helst. Du kan for eksempel se en prosentandel av filene som er blitt arkivert, størrelsen på dataene som holdes under oppsikt, størrelsen på dataen som er arkivert, og størrelsen på dataene som holdes under oppsikt, men som ikke er arkivert ennå. Du kan også se dato for nyeste eller neste arkivering.

Slik viser du et sammendrag av sikkerhetskopieringsaktiviteten:

1. Klikk på kategorien **Lokal arkivering**.
2. Øverst på skjermen klikker du på **Kontosammendrag**.

KAPITTEL 37

McAfee QuickClean

QuickClean forbedrer datamaskinens yteevne ved å slette filer som kan skape rot på datamaskinen. Programmet tømmer papirkurven og sletter midlertidige filer, snarveier, tapte filfragmenter, registerfiler, hurtiglagrede filer, informasjonskapsler, loggfiler i webleseren, sendt og slettet e-post, nylig brukte filer, Active-X-filer og filer med systemgjenopprettingspunkter. QuickClean ivaretar dessuten personvernet ved å bruke McAfee Shredder-programmet til trygt og permanent å slette elementer som kan inneholde følsomme personopplysninger som navn og adresse. Se McAfee Shredder for å lese mer om makulering av filer.

Diskdefragmentering rydder i filer og mapper på datamaskinen for å sikre at de ikke blir spredt (dvs. fragmentert) når de lagres på datamaskinens harddisk. Med regelmessig defragmentering av harddisken kan disse fragmenterte filene og mappene raskt hentes frem igjen senere.

Ønsker du ikke å vedlikeholde datamaskinen manuelt, er det mulig å planlegge det slik at både QuickClean og diskdefragmenteringen går automatisk og uavhengig uansett hyppighet.

Merknad: SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer så snart det oppdager dem. Hvis du trenger hjelp til å diagnostisere beskyttelsesproblemene, kan du kjøre McAfee Virtual Technician.

I dette kapitlet

QuickClean-funksjoner 194
Rens av datamaskinen 195
Defragmentering av datamaskinen 198
Planlegging av oppgave 199

QuickClean-funksjoner

QuickClean inneholder flere rensefunksjoner som sørger for trygg og virkningsfull sletting av unødvendige filer. Plassen på datamaskinens harddisk blir dermed større og yteevnen bedre.

Rens av datamaskinen

QuickClean sletter filer som kan medføre rot på datamaskinen. Programmet tømmer papirkurven og sletter midlertidige filer, snarveier, tapte filfragmenter, registerfiler, hurtiglagrede filer, informasjonskapsler, loggfiler i webleseren, sendt og slettet e-post, nylig brukte filer, Active-X-filer og filer med systemgjenopprettingspunkter. QuickClean sletter disse elementene uten at det får betydning for annen sentral informasjon.

Alle rensefunksjonene i QuickClean kan brukes til å slette unødvendige filer fra datamaskinen. Følgende tabell beskriver rensefunksjonene i QuickClean:

Navn	Funksjon
Papirkurvrens	Sletter filer i papirkurven.
Rens for midlertidige filer	Sletter filer som er lagret i midlertidige mapper.
Snarveirens	Sletter ødelagte snarveier eller snarveier uten tilknyttet program.
Rens for tapte filfragmenter	Sletter tapte filfragmenter på datamaskinen.
Registerrens	Sletter registerinformasjon i Windows® for programmer som ikke lenger finnes på maskinen. Registeret er en database der Windows lagrer konfigurasjonsinformasjon. Registeret inneholder profiler for hver datamaskinbruker og informasjon om maskinvare, installerte programmer og egenskapsinnstillinger. Windows forsyner denne informasjonen med kontinuerlige henvisninger mens systemet kjører.
Hurtiglagerrens	Sletter hurtiglagrede filer som hoper seg opp under Internett-surfing. Disse filene lagres vanligvis som midlertidige filer i en hurtiglagermappe. En hurtiglagermappe er et midlertidig lagringsområde på datamaskinen. Nettleseren kan hente en webside fra hurtiglageret (i stedet for en ekstern server) neste gang siden skal åpnes, og dermed sørge for raskere og mer virkningsfull navigering.

Informasjonskapselrens	Sletter informasjonskapsler. Disse filene er som regel lagret som midlertidige filer. En informasjonskapsel er en liten fil som inneholder informasjon, vanligvis med brukernavn og gjeldende dato og klokkeslett, som en person som navigerer på nettet, har lagret på maskinen. Informasjonskapsler brukes i all hovedsak av webområder til å identifisere brukere som tidligere har registrert seg på eller besøkt området, men de kan også være en kilde til informasjon for hackere.
Loggrens	Sletter loggen i webleseren.
Rens av Outlook Express og Outlook E-mail (sendte og slettede elementer):	Sletter sendt og slettet e-post fra Outlook® og Outlook Express.
Nylig brukt rens	Sletter nylig brukte filer som er opprettet med et av disse programmene: ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Windows History ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®
ActiveX-rens	Sletter ActiveX-kontroller. Active X er en programvarekomponent som programmer eller websider bruker til å tilføye funksjonalitet som glir inn og fremstår som en normal del av programmet eller websiden. De fleste ActiveX-kontrollene er harmløse, men noen kan innhente informasjon fra datamaskinen.
Rens for systemgjenoppretting spunkt	Sletter gamle systemgjenopprettingspunkter (bortsett fra de nyeste) fra datamaskinen. Windows oppretter systemgjenopprettingspunkter for å markere endringer på datamaskinen. Datamaskinen kan dermed gå tilbake til en tidligere tilstand hvis det oppstår problemer.

Rens av datamaskinen

Alle rensefunksjonene i QuickClean kan brukes til å slette unødvendige filer fra datamaskinen. Etterpå er det under **Sammendrag av QuickClean** mulig å vise hvor mye diskplass som er igjen etter rensen, hvor mange filer som ble slettet, og dato og klokkeslett for når QuickClean sist ble kjørt på maskinen.

1. Klikk på **Vedlikehold datamaskin** under **Vanlige oppgaver** i "McAfee SecurityCenter"-ruten.
2. Klikk på **Start** under **MacAfee QuickClean**.
3. Gjør ett av følgende:
   - Klikk på **Neste** for å godta standardrensefunksjonene i listen.
   - Velg eller fjern de ønskede rensefunksjonene, og klikk deretter på **Neste.** Hvis "Nylig brukt rensefunksjon" velges, er det mulig å klikke på **Egenskaper** for å velge eller fjerne filene som nylig ble opprettet med programmene i listen, og deretter klikke på **OK**.
   - Klikk på **Gjenopprett standardinnstillingene** for å gjenopprette standardrensefunksjonene, og klikk deretter på **Neste**.
4. Klikk på **Neste** når analysen er fullført.
5. Klikk på **Neste** for å bekrefte filslettingen.
6. Gjør ett av følgende:
   - Klikk på **Neste** for å godta standardvalget **Nei, jeg vil slette filene med standard Windows-sletting**.
   - Klikk på **Ja, jeg vil utføre sikker fjerning med Shredder**, oppgi antall omganger (opptil 10) og klikk deretter på **Neste**. Det kan ta lang tid å makulere filer hvis mye informasjon er slettet.
7. Hvis filer eller elementer var låst under rensen, kan det hende datamaskinen må startes på nytt. Klikk på **OK** for å lukke meldingen.
8. Klikk på **Fullfør**.

Merknad: Filer som slettes med Shredder, kan ikke gjenopprettes. Se McAfee Shredder for å lese mer om makulering av filer.

Defragmentering av datamaskinen

Diskdefragmentering rydder i filer og mapper på datamaskinen for å sikre at de ikke blir spredt (dvs. fragmentert) når de lagres på datamaskinens harddisk. Med regelmessig defragmentering av harddisken kan disse fragmenterte filene og mappene raskt hentes frem igjen senere.

Defragmentering av datamaskinen

Datamaskinen kan defragmenteres, slik at det blir bedre tilgang til filer og mapper.

1. Klikk på **Vedlikehold datamaskin** under **Vanlige oppgaver** i "McAfee SecurityCenter"-ruten.
2. Klikk på **Analyser** under **Diskdefragmentering** .
3. Følg instruksene på skjermen.

Merknad: Se Windows-hjelpen for å lese mer om diskdefragmentering.

Planlegging av oppgave

Oppgaveplanlegging sørger for at det går automatikk i hvor ofte QuickClean eller diskdefragmenteringen kjøres på maskinen. Eksempelvis kan det planlegges at en QuickClean-oppgave skal tømme papirkurven hver søndag kl. 9.00 eller at en diskdefragmenteringsoppgave skal gå gjennom harddisken siste dag i hver måned. Oppgaver kan opprettes, endres eller slettes når som helst. Det er nødvendig å være logget på datamaskinen for at en planlagt oppgave skal kjøres. Hvis en oppgave av en eller annen grunn ikke kjøres, blir den planlagt på nytt fem minutter etter neste pålogging.

Planlegging av QuickClean-oppgave

QuickClean-oppgaver kan planlegges slik at de automatisk renser datamaskinen med én eller flere rensefunksjoner. Når oppgaven er ferdig, er det under **Sammendrag av QuickClean** mulig å vise dato og klokkeslett for neste gang det er planlagt å kjøre oppgaven.

1 Åpne "Oppgaveplanlegging"-ruten.

   Hvordan?

   1. Klikk på **Vedlikehold datamaskin** under **Vanlige oppgaver** i "McAfee SecurityCenter"-ruten.
   2. Klikk på **Start** under **Oppgaveplanlegging** .

2 Klikk på **McAfee QuickClean** i **Velg operasjon du ønsker å planlegge**-listen.

3 Legg inn navn på oppgaven i **Oppgavenavn**-boksen, og klikk deretter på **Opprett**.

4 Gjør ett av følgende:

   - Klikk på **Neste** for å godta rensefunksjonene i listen.
   - Velg eller fjern de ønskede rensefunksjonene, og klikk deretter på **Neste**. Hvis "Nylig brukt rensefunksjon" velges, er det mulig å klikke på **Egenskaper** for å velge eller fjerne filene som nylig ble opprettet med programmene i listen, og deretter klikke på **OK**.
   - Klikk på **Gjenopprett standardinnstillingene** for å gjenopprette standardrensefunksjonene, og klikk deretter på **Neste**.

5 Gjør ett av følgende:

   - Klikk på **Planlegg** for å godta standardalternativet **Nei, jeg vil slette filene med standard Windows-sletting**.

- Klikk på **Ja, jeg vil utføre sikker fjerning med Shredder**, oppgi antall omganger (opptil 10) og klikk deretter på **Planlegg**.

6 Velg hvor ofte oppgaven skal kjøres i dialogboksen **Planlegg**, og klikk deretter på **OK**.

7 Hvis egenskapene for "Nylig brukte rensefunksjoner" ble endret, kan det hende at datamaskinen må startes på nytt. Klikk på **OK** for å lukke meldingen.

8 Klikk på **Fullfør**.

Merknad: Filer som slettes med Shredder, kan ikke gjenopprettes. Se McAfee Shredder for å lese mer om makulering av filer.

Endring av QuickClean-oppgave

Planlagte QuickClean-oppgaver kan endres slik at andre rensefunksjoner brukes, eller slik at oppgaven ikke kjøres like ofte på maskinen. Når oppgaven er ferdig, er det under **Sammendrag av QuickClean** mulig å vise dato og klokkeslett for neste gang det er planlagt å kjøre oppgaven.

1 Åpne "Oppgaveplanlegging"-ruten.

Hvordan?

1. Klikk på **Vedlikehold datamaskin** under **Vanlige oppgaver** i "McAfee SecurityCenter"-ruten.
2. Klikk på **Start** under **Oppgaveplanlegging** .

2 Klikk på **McAfee QuickClean** i **Velg operasjon du ønsker å planlegge**-listen.

3 Velg oppgave i **Velg en eksisterende oppgave**-listen, og klikk deretter på **Endre**.

4 Gjør ett av følgende:

- Klikk på **Neste** for å godta rensefunksjonene som er valgt til oppgaven.
- Velg eller fjern de ønskede rensefunksjonene, og klikk deretter på **Neste**. Hvis "Nylig brukt rensefunksjon" velges, er det mulig å klikke på **Egenskaper** for å velge eller fjerne filene som nylige ble opprettet med programmene i listen, og deretter klikke på **OK**.
- Klikk på **Gjenopprett standardinnstillingene** for å gjenopprette standardrensefunksjonene, og klikk deretter på **Neste**.

5 Gjør ett av følgende:

- Klikk på **Planlegg** for å godta standardalternativet **Nei, jeg vil slette filene med standard Windows-sletting**.

- Klikk på **Ja, jeg vil utføre sikker fjerning med Shredder**, oppgi antall omganger (opptil 10) og klikk deretter på **Planlegg**.

6 Velg hvor ofte oppgaven skal kjøres i dialogboksen **Planlegg**, og klikk deretter på **OK**.

7 Hvis egenskapene for "Nylig brukte rensefunksjoner" ble endret, kan det hende at datamaskinen må startes på nytt. Klikk på **OK** for å lukke meldingen.

8 Klikk på **Fullfør**.

Merknad: Filer som slettes med Shredder, kan ikke gjenopprettes. Se McAfee Shredder for å lese mer om makulering av filer.

Sletting av QuickClean-oppgave

Planlagte QuickClean-oppgaver kan slettes hvis de ikke lenger skal kjøre automatisk.

1 Åpne "Oppgaveplanlegging"-ruten.

Hvordan?

1. Klikk på **Vedlikehold datamaskin** under **Vanlige oppgaver** i "McAfee SecurityCenter"-ruten.
2. Klikk på **Start** under **Oppgaveplanlegging** .

2 Klikk på **McAfee QuickClean** i **Velg operasjon du ønsker å planlegge**-listen.

3 Velg oppgave i **Velg en eksisterende oppgave**-listen.

4 Klikk på **Slett** og deretter **Ja** for å bekrefte slettingen.

5 Klikk på **Fullfør**.

Planlegging av diskdefragmenteringsoppgave

Det er mulig å planlegge hvor ofte diskdefragmenteringsoppgaver skal kjøres automatisk på datamaskinen. Når oppgaven er ferdig, er det under **Diskdefragmentering** mulig å vise dato og klokkeslett for neste gang det er planlagt å kjøre oppgaven.

1 Åpne "Oppgaveplanlegging"-ruten.

Hvordan?

1. Klikk på **Vedlikehold datamaskin** under **Vanlige oppgaver** i "McAfee SecurityCenter"-ruten.
2. Klikk på **Start** under **Oppgaveplanlegging** .

2 Klikk på **Diskdefragmentering** i **Velg operasjon du ønsker å planlegge**-listen.

3 Legg inn navn på oppgaven i **Oppgavenavn**-boksen, og klikk deretter på **Opprett**.

4 Gjør ett av følgende:

- Klikk på **Planlegg** for å godta standardvalget **Kjør defragmentering selv om det er lite ledig plass**.
- Fjern **Kjør defragmentering selv om det er lite ledig plass**-alternativet, og klikk deretter på **Planlegg**.

5 Velg hvor ofte oppgaven skal kjøres i dialogboksen **Planlegg**, og klikk deretter på **OK**.

6 Klikk på **Fullfør**.

Endring av diskdefragmenteringsoppgave

Det er mulig å endre hvor ofte planlagte diskdefragmenteringsoppgaver skal kjøres automatisk på maskinen. Når oppgaven er ferdig, er det under **Diskdefragmentering** mulig å vise dato og klokkeslett for neste gang det er planlagt å kjøre oppgaven.

1 Åpne "Oppgaveplanlegging"-ruten.

Hvordan?

1. Klikk på **Vedlikehold datamaskin** under **Vanlige oppgaver** i "McAfee SecurityCenter"-ruten.
2. Klikk på **Start** under **Oppgaveplanlegging** .

2 Klikk på **Diskdefragmentering** i **Velg operasjon du ønsker å planlegge**-listen.

3 Velg oppgave i **Velg en eksisterende oppgave**-listen, og klikk deretter på **Endre**.

4 Gjør ett av følgende:

- Klikk på **Planlegg** for å godta standardvalget **Kjør defragmentering selv om det er lite ledig plass**.
- Fjern **Kjør defragmentering selv om det er lite ledig plass**-alternativet, og klikk deretter på **Planlegg**.

5 Velg hvor ofte oppgaven skal kjøres i dialogboksen **Planlegg**, og klikk deretter på **OK**.

6 Klikk på **Fullfør**.

Sletting av diskdefragmenteringsoppgave

Planlagte diskdefragmenteringsoppgaver kan slettes hvis de ikke lenger skal kjøres automatisk.

1. Åpne "Oppgaveplanlegging"-ruten.

   Hvordan?

   1. Klikk på **Vedlikehold datamaskin** under **Vanlige oppgaver** i "McAfee SecurityCenter"-ruten.
   2. Klikk på **Start** under **Oppgaveplanlegging** .

2. Klikk på **Diskdefragmentering** i **Velg operasjon du ønsker å planlegge**-listen.
3. Velg oppgave i **Velg en eksisterende oppgave**-listen.
4. Klikk på **Slett** og deretter **Ja** for å bekrefte slettingen.
5. Klikk på **Fullfør**.

KAPITTEL 38

McAfee Shredder

McAfee Shredder sletter (eller makulerer) elementer permanent og fjerner dem fra datamaskinens harddisk. Selv når man sletter filer og mapper manuelt, tømmer papirkurven eller sletter mappen med midlertidige Internett-filer, er det fortsatt mulig å gjenopprette denne informasjonen med kriminaltekniske dataverktøy. Dessuten kan slettede filer gjenopprettes fordi noen programmer lager midlertidige, skjulte kopier av åpne filer. Shredder ivaretar personvernet ved å slette uønskede filer trygt og permanent. Det er viktig å huske på at makulerte filer ikke kan gjenopprettes.

Merknad: SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer så snart det oppdager dem. Hvis du trenger hjelp til å diagnostisere beskyttelsesproblemene, kan du kjøre McAfee Virtual Technician.

I dette kapitlet

Shredder-funksjoner 206
Makulering av filer, mapper og disker 207

Shredder-funksjoner

Shredder sletter elementer fra datamaskinens harddisk slik at den tilknyttede informasjonen ikke kan gjenopprettes. Programmet ivaretar personvernet ved trygt og permanent å slette filer og mapper, elementer i papirkurven og mappen med midlertidige Internett-filer og alt innholdet på datadisker som skrivbare CD-er, eksterne harddisker og disketter.

Makulering av filer, mapper og disker

Shredder sørger for at informasjonen i slettede filer og mapper i papirkurven og i mappen med midlertidige Internett-filer ikke kan gjenopprettes, ikke engang med spesialverktøy. Med Shredder er det mulig å oppgi hvor mange ganger (opptil 10) et element skal makuleres. Jo flere ganger et element makuleres, desto tryggere er filslettingen.

Makulering av filer og mapper

Filer og mapper, deriblant elementer i papirkurven og mappen med midlertidige Internett-filer, kan makuleres og fjernes fra datamaskinens harddisk.

1 Åpne **Shredder**.

   Hvordan?

   1. Klikk på **Avansert meny** under **Vanlige oppgaver** i ruten McAfee SecurityCenter.
   2. Klikk på **Verktøy** i den venstre ruten.
   3. Klikk på **Shredder**.

2 Klikk på **Slette filer og mapper** under **Jeg vil** i "Makuler filer og mapper"-ruten.

3 Klikk på ett av følgende makuleringsnivåer under **Makuleringsnivå**:

   - **Raskt**: Makulerer det eller de valgte elementene én gang.
   - **Omfattende**: Makulerer det eller de valgte elementene 7 ganger.
   - **Egendefinert**: Makulerer det eller de valgte elementene opptil 10 ganger.

4 Klikk på **Neste**.

5 Gjør ett av følgende:

   - Klikk enten på **Innhold i papirkurven** eller **Midlertidige Internett-filer** i **Velg filen(e) du vil makulere**-listen.
   - Klikk på **Bla gjennom**, naviger til filen som skal makuleres, velg den og klikk deretter på **Åpne**.

6 Klikk på **Neste**.

7 Klikk på **Start**.

8 Klikk på **Fullført** når Shredder er ferdig.

Merknad: Ikke arbeid med disse filene før Shredder har fullført oppgaven.

Makulering av hel disk

Det er mulig å slette alt innholdet på en disk i én operasjon. Bare flyttbare stasjoner som eksterne harddisker, skrivbare CD-er og disketter kan makuleres.

1. Åpne **Shredder**.

   Hvordan?

   1. Klikk på **Avansert meny** under **Vanlige oppgaver** i ruten McAfee SecurityCenter.
   2. Klikk på **Verktøy** i den venstre ruten.
   3. Klikk på **Shredder**.

2. Klikk på **Slette en hel disk** under **Jeg vil** i "Makuler filer og mapper"-ruten.
3. Klikk på ett av følgende makuleringsnivåer under **Makuleringsnivå**:
   - **Raskt**: Makulerer den valgte disken én gang.
   - **Omfattende**: Makulerer den valgte disken 7 ganger.
   - **Egendefinert**: Makulerer den valgte disken opptil 10 ganger.
4. Klikk på **Neste**.
5. Klikk på den disken i **Velg disk**-listen som skal makuleres.
6. Klikk på **Neste** og deretter **Ja** for å bekrefte.
7. Klikk på **Start**.
8. Klikk på **Fullført** når Shredder er ferdig.

Merknad: Ikke arbeid med disse filene før Shredder har fullført oppgaven.

KAPITTEL 39

McAfee Network Manager

Network Manager gir en grafisk visning av datamaskinen og komponentene som hjemmenettverket ditt består av. Du kan bruke Network Manager til å overvåke beskyttelsesstatusen på hver administrerte datamaskin i nettverket eksternt, og reparere rapporterte sikkerhetsproblemer på de administrerte datamaskinene eksternt.

Før du begynner å bruke Network Manager, kan du gjøre deg kjent med noen av funksjonene. Du finner mer informasjon om hvordan du konfigurerer og bruker disse funksjonene, i hjelpen for Network Manager.

Merknad: SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer så snart det oppdager dem. Hvis du trenger hjelp til å diagnostisere beskyttelsesproblemene, kan du kjøre McAfee Virtual Technician.

I dette kapitlet

Network Manager funksjoner 210
Forstå Network Manager-ikoner.....211
Sette opp et administrert nettverk 213
Administrere nettverket eksternt 221

Network Manager funksjoner

Network Manager har følgende funksjoner.

Grafisk nettverkskart

Network Managers nettverkskart gir en geografisk oversikt over beskyttelsesstatusen til datamaskinene og komponentene som utgjør hjemmenettverket ditt. Når du foretar endringer i nettverket (for eksempel du legger til en ny datamaskin), gjenkjenner nettverkskartet disse endringene. Du kan oppdatere nettverkskartet, gi nettverket et nytt navn samt vise/skjule komponenter på nettverkskartet for å tilpasse visningen. Du kan også vise detaljer om komponentene som vises på nettverkskartet.

Ekstern administrasjon

Network Managers nettverkskart gir en geografisk oversikt over beskyttelsesstatusen til datamaskinene og komponentene som utgjør hjemmenettverket ditt. Du kan invitere en datamaskin til å koble seg til det administrative nettverket, overvåke den administrerte datamaskinens beskyttelsesstatus samt fikse kjente sikkerhetshull fra en ekstern datamaskin på nettverket.

Forstå Network Manager-ikoner

Den følgende tabellen beskriver ikonene som oftest blir brukt i nettverkskartet i Network Manager.

Ikon	Beskrivelse
	Representerer en administrert datamaskin som er frakoblet
	Representerer en administrert datamaskin som er frakoblet
	Representerer en ikke-administrert datamaskin som har SecurityCenter installert
	Representerer en frakoblet datamaskin som ikke er administrert
	Representerer en tilkoblet datamaskin som ikke har SecurityCenter installert, eller en ukjent nettverksenhet
	Representerer en tilkoblet datamaskin som ikke har SecurityCenter installert, eller en ikke tilkoblet, ukjent nettverksenhet
	Betyr at det tilsvarende elementet er beskyttet og tilkoblet
	Betyr at det tilsvarende elementet kan kreve ditt tilsyn
	Betyr at det tilsvarende elementet krever umiddelbart ditt tilsyn
	Representerer en trådløs ruter
	Representerer en vanlig ruter
	Representerer Internett, når det er tilkoblet
	Representerer Internett, når det er frakoblet

KAPITTEL 40

Sette opp et administrert nettverk

Du kan sette opp et administrert nettverk med elementene på nettverkskartet og legge medlemmer (datamaskiner) til nettverket. Før en datamaskin kan administreres eksternt, eller gis tillatelse til å administrere andre datamaskiner via nettverket, må den bli et klarert medlem av nettverket. Nettverksmedlemskap blir gitt nye datamaskiner av eksisterende nettverksmedlemmer (datamaskiner) med administrative rettigheter.

Du kan vise detaljer om komponentene som vises på nettverkskartet, selv etter at du har foretatt endringer i ditt nettverk (for eksempel lagt til en datamaskin).

I dette kapitlet

Arbeide med nettverkskartet.....214
Koble til det administrerte nettverket.....216

Arbeide med nettverkskartet

Når du kobler en datamaskin til nettverket, analyserer Network Manager nettverkets tilstand for å finne ut om det er noen administrerte eller ikke-administrerte medlemmer tilkoblet, hva ruterens egenskaper er, og Internett-status. Hvis ingen medlemmer er tilkoblet, tar Network Manager utgangspunkt i at den datamaskinen som for øyeblikket er koblet til, er den første datamaskinen i nettverket, og registrerer denne datamaskinen som et administrert medlem med administrative rettigheter. Nettverksnavnet inkluderer som standard navnet på arbeidsgruppen eller domenet til den første datamaskinen som kobler seg til med SecurityCenter installert. Du kan imidlertid gi nettverket et nytt navn når som helst.

Når du endrer noe i nettverket (for eksempel hvis du legger til en datamaskin), kan du tilpasse nettverkskartet. Du kan for eksempel oppdatere nettverkskartet, gi nettverket nytt navn og skjule eller vise komponenter i nettverket for å tilpasse visningen. Du kan også vise detaljer om komponentene som vises på nettverkskartet.

Få tilgang til nettverkskartet

Nettverkskartet gir en grafisk fremstilling av datamaskinene og komponentene som hjemmenettverket ditt består av.

- Klikk **Administrert nettverk** på den grunnleggende eller avanserte menyen.

Merk: Første gang du får tilgang til nettverkskartet, blir du bedt om å stole på de andre datamaskinene i nettverket.

Oppdatere nettverkskartet

Du kan oppdatere nettverkskartet når som helst, for eksempel etter at en annen datamaskin har logget seg på det administrerte nettverket.

1. Klikk **Administrert nettverk** på den grunnleggende eller avanserte menyen.
2. Klikk **Oppdater nettverkskartet** under **Jeg vil**.

Merknad: Oppdater nettverkskartet-koblingen er bare tilgjengelig hvis ingen komponenter er valgt på nettverkskartet. Hvis du vil oppheve valget av et element, klikker du det valgte elementet eller klikker i et blankt område på nettverkskartet.

Gi nettverket nytt navn

Nettverksnavnet inkluderer som standard navnet på arbeidsgruppen eller domenet til den første datamaskinen som kobler seg til nettverket med SecurityCenter installert. Hvis du ønsker å bruke et annet navn, kan du endre det.

1. Klikk **Administrert nettverk** på den grunnleggende eller avanserte menyen.
2. Klikk **Gi nettverket nytt navn** under **Jeg vil**.
3. Skriv inn navnet på nettverket i boksen **Nettverksnavn**.
4. Klikk **OK**.

Merknad: Gi nettverket nytt navn-koblingen er bare tilgjengelig hvis ingen komponenter er valgt på nettverkskartet. Hvis du vil oppheve valget av et element, klikker du det valgte elementet eller klikker i et blankt område på nettverkskartet.

Vise eller skjule et element på nettverkskartet

Alle datamaskiner og komponenter i hjemmenettverket ditt vises på nettverkskartet som standard. Du kan imidlertid vise elementer igjen som du har skjult tidligere. Kun ikke-administrerte elementer kan skjules. Administrerte datamaskiner kan ikke skjules.

For å...	På menyen Grunnleggende eller Avansert klikker **duBehandle nettverk**, og deretter gjør du følgende...
Skjule et element på nettverkskartet	Klikk et element på nettverkskartet og klikk **Skjul dette elementet** under **Jeg vil**. I bekreftelsesdialogboksen klikker du **Ja**.
Vise skjulte elementer på nettverkskartet	Klikk **Vis skjulte elementer** under **Jeg vil**.

Vis detaljer for et element

Du kan vise detaljert informasjon om alle komponenter i nettverket hvis du velger det på nettverkskartet. Denne informasjonen inkluderer komponentnavnet, beskyttelsesstatusen og annen informasjon som er nødvendig for å administrere komponenten.

1. Klikk på elementets ikon på nettverkskartet.
2. Vis informasjonen om elementet under **Detaljer**.

Koble til det administrerte nettverket

Før en datamaskin kan administreres eksternt, eller gis tillatelse til å administrere andre datamaskiner via nettverket, må den bli et klarert medlem av nettverket. Nettverksmedlemskap blir gitt nye datamaskiner av eksisterende nettverksmedlemmer (datamaskiner) med administrative rettigheter. For å sikre at bare klarerte datamaskiner kobler seg til nettverket, må brukeren på datamaskinen som gir tilgang til nettverket, og brukeren på datamaskinen som kobler seg til nettverket, autentifisere hverandre.

Når en datamaskin kobles til nettverket, blir den bedt om å dele sin McAfee-beskyttelsesstatus med de andre datamaskinene i nettverket. Hvis en datamaskin går med på å dele beskyttelsesstatusen sin, blir den et administrert medlem av nettverket. Hvis en datamaskin ikke går med på å dele beskyttelsesstatusen sin, blir den et ikke-administrert medlem av nettverket. Ikke-administrerte nettverksmedlemmer er vanligvis gjestemaskiner som vil ha tilgang til andre nettverksfunksjoner (for eksempel sende filer eller dele skrivere).

Merk: Hvis du har andre McAfee-nettverksprogrammer installert (for eksempel EasyNetwork), blir datamaskinen også gjenkjent som et administrert medlem i disse programmene, etter at du har koblet den til. Tillatelsesnivået som er tildelt en datamaskin i Network Manager, gjelder for alle McAfee-nettverksprogrammer. Hvis du vil ha mer informasjon om hva gjestetilgang, full tilgang eller administrative rettigheter betyr i andre McAfee-nettverksprogrammer, kan du se i dokumentasjonen som følger med programmet.

Koble til et administrert nettverk

Når du får en invitasjon om å koble til et administrert nettverk, kan du godta den eller avslå den. Du kan også avgjøre om du vil at denne og andre datamaskiner i nettverket skal overvåke hverandres sikkerhetsinnstillinger (for eksempel om en datamaskins virusbeskyttelsestjenester er oppdaterte).

1. I dialogboksen til det administrative nettverket, sørg for at boksen**Tillat enhver datamaskin i dette nettverket til å overvåke sikkerhetsinnstillinger** er valgt.
2. Klikk **Koble til**.
   Når du godtar invitasjonen, vises to spillekort.
3. Bekreft at det er de samme spillekortene som vises på datamaskinen, som inviterte deg til å koble til det administrerte nettverket.
4. Klikk **OK**.

Merknad: Hvis datamaskinen som inviterte deg til å koble til det administrative nettverket, ikke viser de samme spillekortene som vises i dialogboksen for sikkerhetsbekreftelse, har det oppstått et sikkerhetsbrudd i det administrative nettverket. Det kan utgjøre en sikkerhetsrisiko for din datamaskin. Klikk **Avbryt** i dialogboksen til det administrative nettverket.

Invitere en datamaskin til å koble seg til det administrerte nettverket

Hvis en datamaskin blir lagt til i det administrerte nettverket, eller hvis det er en annen ikke-administrert datamaskin i nettverket, kan du invitere datamaskinen til å koble seg til det administrerte nettverket. Bare datamaskiner med administrative rettigheter til nettverket kan invitere andre datamaskiner til å koble seg til. Når du sender en invitasjon, spesifiserer du også tillatelsesnivået du ønsker å tildele det nye medlemmet.

1. Klikk på ikonet til den ikke-administrerte datamaskinen på nettverkskartet.
2. Klikk på**Overvåk denne datamaskinen** under **Jeg vil**.
3. I dialogboksen for å invitere en datamaskin til å koble seg til det administrative nettverket gjør du ett av følgende:
   - Klikk på **Gi gjest tilgang til administrerte nettverksprogrammer** for å gi datamaskinen tilgang til nettverket (du kan bruke dette alternativet for midlertidige brukere i ditt hjem).
   - Klikk på **Gi full tilgang til administrerte nettverksprogrammer** for å gi datamaskinen tilgang til nettverket.

- Klikk på **Gi administrative rettigheter til administrerte nettverksprogrammer** for å gi datamaskinen tilgang til nettverket med administrative rettigheter. Datamaskinen kan også gi tilgang til andre datamaskiner som vil bli med i det administrative nettverket.

4 Klikk **OK**.
En invitasjon til å koble til det administrerte nettverket blir sendt til datamaskinen. Når datamaskinen godtar invitasjonen, vises to spillekort.

5 Bekreft at det er de samme spillekortene som vises på datamaskinen du inviterte til å koble seg til det administrerte nettverket.

6 Klikk på**Gi tilgang**.

Merknad: Hvis datamaskinen du inviterte til å koble seg til det administrative nettverket, ikke viser de samme spillekortene som vises i dialogboksen for sikkerhetsbekreftelse, har det oppstått et sikkerhetsbrudd i det administrative nettverket. Det å gi datamaskinen tilgang til å koble til nettverket kan utgjøre en sikkerhetsrisiko for andre datamaskiner. Klikk derfor på **Nekt tilgang** i dialogboksen for sikkerhetsbekreftelse.

Slutte å stole på datamaskiner i nettverket

Hvis du stolte på andre datamaskiner i nettverket ved en feil, kan du stoppe å stole på dem.

- Klikk på**Slutt å stole på datamaskiner i dette nettverket** under **Jeg vil**.

Merk: Koblingen for å slutte å stole på datamaskiner i dette nettverket er ikke tilgjengelig hvis du har administrative rettigheter og det er andre administrerte datamaskiner i nettverket.

KAPITTEL 41

Administrere nettverket eksternt

Etter at du har satt opp et administrert nettverk, kan du administrere eksternt datamaskinene og komponentene som hjemmenettverket ditt består av. Du kan overvåke statusen og tilgangsnivåene til datamaskinene og komponentene, samt løse de fleste sikkerhetshull eksternt.

I dette kapitlet

Overvåke status og tillatelser.....222
Løse sikkerhetshull.....224

Overvåke status og tillatelser

Et administrert nettverk har administrerte og ikke-administrerte medlemmer. Administrerte medlemmer tillater andre datamaskiner i nettverket å overvåke deres McAfee-beskyttelsesstatus. Ikke-administrerte medlemmer gjør ikke det. Ikke-administrerte nettverksmedlemmer er vanligvis gjestemaskiner som vil ha tilgang til andre nettverksfunksjoner (for eksempel sende filer eller dele skrivere). En ikke-administrert datamaskin kan inviteres til å bli en administrert datamaskin når som helst av en annen administrert datamaskin i nettverket. På samme måte kan en administrert datamaskin endre status til ikke-administrert når som helst.

Administrerte datamaskiner har administrative rettigheter, full tilgang eller gjestetilgang. Administrative rettigheter gjør at den administrerte datamaskinen kan overvåke beskyttelsesstatusen til alle administrerte datamaskiner i nettverket, og gi andre datamaskiner tilgang til nettverket. Full tilgang og gjestetilgang gir kun datamaskinen tilgang til nettverket. Du kan endre tillatelsesnivået til en datamaskin når som helst.

Siden et administrert nettverk også kan ha enheter (for eksempel rutere), kan du bruke Network Manager til å administrere disse enhetene. Du kan også konfigurere og endre egenskapene til en enhet på nettverkskartet.

Overvåke beskyttelsesstatusen til en datamaskin

Hvis en datamaskins beskyttelsesstatus ikke blir overvåket på nettverket (datamaskinen er ikke et medlem, eller er et ikke-administrert medlem), kan du be om å overvåke den.

1. Klikk på ikonet til den ikke-administrerte datamaskinen på nettverkskartet.
2. Klikk på**Overvåk denne datamaskinen** under **Jeg vil**.

Slutte å overvåke beskyttelsesstatusen til en datamaskin

Du kan slutte å overvåke beskyttelsesstatusen til en administrert datamaskin i ditt private nettverk. Datamaskinen blir da ikke administrert og du kan ikke overvåke beskyttelsesstatusen eksternt.

1. Klikk på ikonet til den administrerte datamaskinen på nettverkskartet.
2. Klikk på **Stopp overvåkning av denne datamaskinen** under **Jeg vil**.
3. I bekreftelsesdialogboksen klikker du **Ja**.

Endre tillatelsene til en administrert datamaskin

Du kan endre tillatelsene til en datamaskin når som helst. Dette gjør at du kan justere hvilke datamaskiner som kan overvåke beskyttelsesstatusen til andre datamaskiner i nettverket.

1. Klikk på ikonet til den administrerte datamaskinen på nettverkskartet.
2. Klikk på **Endre tillatelser for denne datamaskinen** under **Jeg vil**.
3. I dialogboksen for endring av tillatelser markerer eller fjerner du avmerkingen av boksen for å angi om denne og andre datamaskiner i det administrerte nettverket kan overvåke hverandres beskyttelsesstatus.
4. Klikk **OK**.

Administrere en enhet

Du kan behandle en enhet ved å åpne administrasjonswebsiden fra Network Manager.

1. Klikk på enhetens ikon på nettverkskartet.
2. Klikk på**Behandle denne enheten** under **Jeg vil**.
   En webleser åpnes og viser enhetens administrasjonswebside.
3. Oppgi påloggingsinformasjon og konfigurer enhetens sikkerhetsinnstillinger i webleseren.

Merk: Hvis enheten er en trådløs ruter eller et tilgangspunkt som er beskyttet av Wireless Network Security, må du bruke Wireless Network Security til å konfigurere sikkerhetsinnstillingene for enheten.

Endre visningsegenskapene til en enhet

Når du endrer visningsegenskapene til en enhet, kan du endre enhetens visningsnavn på nettverkskartet og spesifisere om enheten er en trådløs ruter.

1. Klikk på enhetens ikon på nettverkskartet.
2. Klikk på **Endre enhetens egenskaper** under **Jeg vil**.
3. Skriv inn et navn i **Navn**-boksen for å spesifisere visningsnavnet for enheten.
4. Hvis du vil spesifisere enhetstype, klikk på **Standard Ruter** dersom den ikke er en trådløs ruter, eller **Trådløs Ruter** dersom den er trådløs.
5. Klikk **OK**.

Løse sikkerhetshull

Administrerte datamaskiner med administrative rettigheter kan overvåke McAfee-beskyttelsesstatusen til andre administrerte datamaskiner i nettverket, og løse eventuelle innrapporterte sikkerhetshull eksternt. Hvis for eksempel McAfee-beskyttelsesstatusen til en administrert datamaskin viser at VirusScan er deaktivert, kan en annen administrert datamaskin med administrative rettigheter aktivere VirusScan eksternt.

Når du løser sikkerhetshull eksternt, løser Network Manager de fleste rapporterte problemer. Noen sikkerhetshull krever imidlertid manuell inngripen på den lokale maskinen. I dette tilfellet løser Network Manager de problemene som kan løses eksternt, og ber deg deretter løse de gjenværende problemene ved å logge deg på SecurityCenter på den utsatte maskinen og følge de anbefalingene som blir gitt. I noen tilfeller er den anbefalte løsningen på problemet å installere den siste versjonen av SecurityCenter på den eksterne maskinen eller på datamaskiner i nettverket.

Løse sikkerhetshull

Du kan bruke Network Manager til å løse de fleste sikkerhetshull på eksterne, administrerte datamaskiner. For eksempel, hvis VirusScan er deaktivert på en ekstern datamaskin, kan du aktivere den.

1. Klikk på elementets ikon på nettverkskartet.
2. Vis beskyttelsesstatusen til elementet under **Detaljer**.
3. Klikk på **Reparer sikkerhetshull** under **Jeg vil**.
4. Når sikkerhetshull har blitt løst, klikker du på **OK**.

Merk: Selv om Network Manager løser de fleste sikkerhetshull automatisk, krever noen reparasjoner at du åpner SecurityCenter på den utsatte datamaskinen og følger de anbefalingene som blir gitt.

Installere McAfee-sikkerhetsprogramvare på eksterne datamaskiner

Hvis en eller flere datamaskiner i nettverket ikke bruker siste versjon av SecurityCenter, kan ikke beskyttelsesstatusen deres overvåkes eksternt. Hvis du ønsker å overvåke disse datamaskinene eksternt, må du gå til hver enkelt datamaskin og installere siste versjon av SecurityCenter.

1. Åpne SecurityCenter på datamaskinen du vil installere sikkerhetsprogrammet på.
2. Under **Vanlige oppgaver** klikker du **Min konto**.
3. Logg på med e-postadressen og passordet du brukte til å registrere sikkerhetsprogrammet første gang du installerte det.
4. Velg ønsket produkt, klikk **Last ned / Installer**, og følg deretter instruksjonene på skjermen.

KAPITTEL 42

McAfee EasyNetwork

Med Easy Network får du sikker fildeling, enkel filoverføring og alle datamaskinene i hjemmenettverket får tilgang til skriveren. Imidlertid må datamaskinene i ditt nettverk ha EasyNetwork installert for å ha tilgang til dets funksjoner.

Før du begynner å bruke EasyNetwork, kan du gjøre deg kjent med noen av funksjonene. EasyNetwork-hjelp har informasjon om å konfigurere og bruke disse funksjonene.

Merknad: SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer så snart det oppdager dem. Hvis du trenger hjelp til å diagnostisere beskyttelsesproblemene, kan du kjøre McAfee Virtual Technician.

I dette kapitlet

EasyNetwork funksjoner....228
Konfigurere EasyNetwork....229
Dele og sende filer....235
Dele skrivere....241

EasyNetwork funksjoner

EasyNetwork har følgende funksjoner.

Fildeling

EasyNetwork gjør det enkelt å dele filer med andre datamaskiner i ditt nettverk. Når du deler filer, gir du de andre datamaskinene lesetilgang til disse filene. Kun datamaskiner som har full eller administrativ tilgang til ditt administrative nettverk (medlemmer), kan dele eller få tilgang til filer som deles av andre medlemmer.

Filoverføring

Du kan sende filer til andre datamaskiner som har full eller administrativ tilgang til ditt administrative nettverk (medlemmer). Når du mottar en fil, vises den i EasyNetwork-innboksen. Innboksen er en midlertidig lagringsplass for alle filene som sendes til deg fra andre datamaskiner i nettverket.

Automatisk skriverdeling

Når du blir med i et administrativt nettverk, kan du dele lokale skrivere som er koblet til datamaskinen din med andre medlemmer, og bruke skriverens gjeldende navn som det delte skrivernavnet. Den oppdager også skrivere som deles av andre datamaskiner på nettverket, og tillater deg å konfigurere og bruke disse skriverne.

KAPITTEL 43

Konfigurere EasyNetwork

Før du kan bruke EasyNetwork, må du åpne den og koble deg til et administrativt nettverk. Etter at du har koblet deg til et administrativt nettverk, kan du dele, søke etter, og sende filer til andre datamaskiner i nettverket. Du kan også dele skrivere. Dersom du bestemmer deg for å forlate nettverket, kan du gjøre dette når som helst.

I dette kapitlet

Åpne EasyNetwork 229
Logge seg på et administrativt nettverk 230
Forlate et administrativt nettverk 234

Åpne EasyNetwork

Du blir som standard bedt om å åpne EasyNetwork rett etter at du har installert programmet, men du kan også åpne EasyNetwork senere.

- Gå til **Start**-menyen, velg **Programmer**, velg **McAfee**, og klikk deretter på **McAfee EasyNetwork**.

Tips: Hvis du opprettet ikoner på skrivebordet samt hurtigtastikoner under installasjonen, kan du også åpne EasyNetwork ved å dobbeltklikke på McAfee EasyNetwork-ikonet på skrivebordet eller klikke på McAfee EasyNetwork-ikonet i systemstatusfeltet helt til høyre for oppgavelinjen.

Logge seg på et administrativt nettverk

Hvis ingen datamaskiner i nettverket som du er koblet til har SecurityCenter, blir du medlem av nettverket og du blir spurt om nettverket er til å stole på. Hvis du er den første datamaskinen som blir med i nettverket, blir ditt datamaskinnavn med i nettverksnavnet. Du kan imidlertid endre navnet når som helst.

Når en datamaskin kobles til nettverket, sender den en påloggingsanmodning til de andre datamaskinene som er koblet til nettverket. Alle datamaskiner med administrative rettigheter i nettverket, kan gi tilgang. Godkjenneren kan også bestemme tillatelsesnivået til datamaskinen som ble koblet til nettverket, for eksempel gjest (kun filoverføring) eller full tilgang / administrativ (filoverføring og fildeling). Med EasyNetwork kan datamaskiner med administrative rettigheter gi tilgang til andre datamaskiner og administrere tillatelser (tillate eller ikke tillate). Datamaskiner med full tilgang kan ikke utføre disse administrative oppgavene.

Merk: Hvis du har andre McAfee-nettverksprogrammer installert (for eksempel Network Manager), blir datamaskinen også gjenkjent som et administrert medlem i disse programmene, etter at du har koblet den til. Tillatelsesnivået som angis til en datamaskin i EasyNetwork, gjelder for alle McAfees nettverksprogrammer. Hvis du vil ha mer informasjon om hva gjestetilgang, full tilgang eller administrative rettigheter betyr i andre McAfee-nettverksprogrammer, kan du se i dokumentasjonen som følger med programmet.

Logge på nettverket

Når en datamaskin kobler seg på et pålitelig nettverk for første gang etter at EasyNetwork er installert, vises en melding der du blir spurt om du vil logge deg på det administrative nettverket. Hvis datamaskinen godtar å logge seg på, sendes en anmodning til alle de andre nettverksdatamaskinene som har administrativ tilgang. Denne anmodningen må innvilges før datamaskinen kan dele skrivere eller filer, eller sende og kopiere filer på nettverket. Den første datamaskinen i nettverket blir automatisk gitt administrative rettigheter.

1. I vinduet for delte filer, klikker du på **Logg på dette nettverket**.
   Når en administrativ datamaskin i nettverket gir deg tilgang, vises en melding der du blir spurt om du vil la denne datamaskinen og andre datamaskiner i nettverket administrere hverandres sikkerhetsinnstillinger.
2. Hvis du vil la denne datamaskinen og andre datamaskiner i nettverket administrere hverandres sikkerhetsinnstillinger, klikker du på **OK**. I motsatt tilfelle klikker du på **Avbryt**.
3. Bekreft at datamaskinen viser spillekortene som vises i dialogboksen for sikkerhetsbekreftelse, og klikk deretter på **OK**.

Merknad: Hvis datamaskinen som inviterte deg til å koble til det administrative nettverket, ikke viser de samme spillekortene som vises i dialogboksen for sikkerhetsbekreftelse, har det oppstått et sikkerhetsbrudd i det administrative nettverket. Det kan utgjøre en sikkerhetsrisiko for din datamaskin. Klikk **Avbryt** i dialogboksen for sikkerhetsbekreftelse.

Gi tilgang til nettverket

Når en datamaskin anmoder om å logge seg på det administrative nettverket, sendes en melding til alle de andre nettverksdatamaskinene som har administrativ tilgang. Den første datamaskinen som svarer, blir godkjenneren. Når du er godkjenner, har du ansvaret for hvilken tilgangstype datamaskinen skal få: gjestetilgang, full tilgang eller administrativ tilgang.

1. Velg egnet tilgangsnivåer.
2. I dialogboksen for å invitere en datamaskin til å koble seg til det administrative nettverket gjør du ett av følgende:
   - Klikk på **Gi gjest tilgang til administrerte nettverksprogrammer** for å gi datamaskinen tilgang til nettverket (du kan bruke dette alternativet for midlertidige brukere i ditt hjem).
   - Klikk på **Gi full tilgang til administrerte nettverksprogrammer** for å gi datamaskinen tilgang til nettverket.

- Klikk på **Gi administrative rettigheter til administrerte nettverksprogrammer** for å gi datamaskinen tilgang til nettverket med administrative rettigheter. Datamaskinen kan også gi tilgang til andre datamaskiner som vil bli med i det administrative nettverket.

3 Klikk **OK**.

4 Bekreft at datamaskinen viser spillekortene som vises i dialogboksen for sikkerhetsbekreftelse, og klikk deretter på **Gi Tilgang**.

Merk: Hvis datamaskinen ikke viser de samme spillekortene som vises i dialogboksen for sikkerhetsbekreftelse, har det oppstått et sikkerhetsbrudd på det administrative nettverket. Det kan være risikofylt å gi denne datamaskinen tilgang til nettverket, så du bør klikke på **Avvis** i dialogboksen for sikkerhetsbekreftelse.

Gi nettverket nytt navn

Nettverksnavnet inkluderer som standard navnet på den første datamaskinen som ble med i nettverket. Du kan imidlertid endre navnet når som helst. Når du gir nettverket et nytt navn, endrer du nettverksbeskrivelsen som vises i EasyNetwork.

1. Klikk på **Konfigurer** på **Alternativer**-menyen.
2. I konfigurasjonsboksen skriver du inn navnet på nettverket i boksen **Nettverksnavn**.
3. Klikk **OK**.

Forlate et administrativt nettverk

Hvis du logger deg på et administrativt nettverk men så bestemmer deg for ikke å være medlem, kan du forlate nettverket. Etter at du forlater det administrative nettverket, kan du alltid bli med igjen, men da må du få tillatelse til å logge deg på igjen. Du finner mer informasjon om å logge seg på i Logge seg på et administrativt nettverk (side 230).

Forlate et administrativt nettverk

Du kan forlate et administrativt nettverk som du tidligere logget deg på.

1. Klikk på **Forlat nettverk** i **Verktøy**-menyen.
2. I Forlat nettverk-dialogboksen velger du navnet på nettverket du vil forlate.
3. Klikk på **Forlat nettverk**.

KAPITTEL 44

Dele og sende filer

EasyNetwork gjør det enkelt å dele og sende filer til andre datamaskiner på nettverket. Når du deler filer, gir du de andre datamaskinene lesetilgang til disse. Kun datamaskiner som er medlemmer av det administrative nettverket (full eller administrativ tilgang), kan dele eller få tilgang til filer som deles av andre datamaskiner.

Merknad: Hvis du deler et stort antall av filer, kan ressursene til din datamaskin bli påvirket.

I dette kapitlet

Dele filer 236
Sende filer til andre datamaskiner 239

Dele filer

Kun datamaskiner som er medlemmer av det administrative nettverket (full eller administrativ tilgang), kan dele eller få tilgang til filer som deles av andre datamaskiner. Hvis du deler en mappe, deles alle filene i den mappen og eventuelle undermapper. Filer som senere legges i den mappen, blir imidlertid ikke automatisk delt. Hvis en delt fil eller mappe slettes, fjernes den fra vinduet for delte filer. Du kan slutte å dele en fil når som helst.

Hvis du vil ha tilgang til en delt fil, åpne filen direkte fra EasyNetwork eller kopier den til din datamaskin, og så åpne den derfra. Hvis listen over delte filer blir lang og det vanskelig å se hvor filen er, kan du søke etter den.

Merknad: Andre datamaskiner som bruker Window Explorer, har ikke tilgang til filer som deles via EasyNetwork. Fildeling med EasyNetwork må foregå over sikre tilkoblinger.

Dele filer

Når du deler en fil, blir den tilgjengelig for alle medlemmer som har full eller administrativ tilgang til det administrative nettverket.

1. Finn filen du vil dele, i Windows Utforsker.
2. Dra filen fra Windows Utforsker til vinduet for delte filer i EasyNetwork.

Tips: Du kan også dele en fil dersom du klikker på **Dele filer** i **Verktøy**-menyen. I Dele-dialogboksen finner du filen du vil dele, velger den og klikker på **Dele**.

Stanse deling av fil

Hvis du deler en fil på det administrative nettverket, kan du stanse delingen når som helst. Når du stanser delingen av en fil, har ikke andre medlemmer av det administrative nettverket tilgang.

1. Klikk på **Stanse deling av filer** i **Verktøy**-menyen.
2. I dialogboksen for stans av fildeling velger du den filen du ikke lenger vil dele.
3. Klikk **OK**.

Kopiere en delt fil

Du kan kopiere en delt fil slik at du fortsatt har den når den ikke deles lenger. Du kan kopiere en delt fil fra enhver datamaskin i ditt administrative nettverk.

- Dra filen fra vinduet for delte filer i EasyNetwork til et sted på Windows Utforsker eller Windows Skrivebord.

Tips: Du kan også kopiere en delt fil dersom du velger filen i EasyNetwork, og deretter klikker på **Kopi til** på **Verktøy**-menyen. I Kopi til-dialogboksen navigerer du til mappen du vil kopiere filen til, velger den og klikker på **Lagre**.

Søke etter en delt fil

Du kan søke etter en fil som er delt av deg eller andre nettverksmedlemmer. Når du skriver inn søkekriteriene, viser EasyNetwork resultatet i vinduet for delte filer.

1. Klikk på **Søk** i vinduet for delte filer.
2. Klikk på ønsket alternativ (side 237) i listen **Innehold**.
3. Skriv inn hele eller deler av filnavnet eller banen i listen **Fil- eller banenavn**.
4. Klikk på ønsket filtype (side 237) i listen **Type**.
5. I listene **Fra** og **Til** klikker du på datoene som representerer når filen ble opprettet.

Søkekriterier

Følgende tabeller beskriver de søkekriterier som du kan oppgi når du søker etter delte filer.

Navn på filen eller bane

Inneholder:	Beskrivelse
Inneholder alle ordene	Søk etter en fil eller banenavn som inneholder alle ordene du har oppgitt i listen **Fil- eller banenavn**.
Inneholder et hvilket som helst av ordene	Søker etter en fil eller banenavn som inneholder ett eller flere av ordene du har oppgitt i **Fil- eller banenavn**-listen.
Inneholder nøyaktig streng	Søker etter en fil eller banenavn som inneholder den nøyaktige frasen du oppgav i **Fil- eller banenavn**-listen.

Filtype

Type	Beskrivelse
Alle	Søker alle delte filtyper.
Dokument	Søker alle delte dokumenter.
Bilde	Søker alle delte bildefiler.
Video	Søker alle delte videofiler.
Lyd	Søker alle delte lydfiler.
Komprimert	Søke alle komprimerte filer (for eksempel ZIP-filer).

Sende filer til andre datamaskiner

Du kan sende filer til andre datamaskiner som er medlemmer av det administrative nettverket. Før du sender en fil, bekrefter EasyNetwork at datamaskinen som skal motta filen, har nok tilgjengelig lagringsplass.

Når du mottar en fil, vises den i EasyNetwork-innboksen. Innboksen er en midlertidig lagringsplass for filer som sendes til deg fra andre datamaskiner i nettverket. Hvis EasyNetwork er åpen når du mottar en fil, vises filen øyeblikkelig i innboksen. Ellers vises en melding i systemstatusfeltet helt til høyre for din oppgavelinje. Hvis du ikke vil motta meldingen (for eksempel da de forstyrrer det du foretar deg), kan du skru denne funksjonen av. Hvis innboksen allerede har en fil med samme navn, får den nye filen et nytt navn med numerisk endelse. Filer blir i innboksen til du godtar dem (kopierer dem til datamaskinen din).

Sende en fil til en annen datamaskin

Du kan sende en fil til en annen datamaskin på det administrative nettverket uten å dele den. Før mottakeren kan se filen, må den lagres lokalt. Du finner mer informasjon i Godta en fil fra en annen datamaskin (side 239).

1. Finn filen du vil sende, i Windows Utforsker.
2. Dra filen fra Windows Utforsker til et aktivt dataikon i EasyNetwork.

Tips: Flere filer kan sendes til en datamaskin ved å trykke på CTRL-knappen når du velger filene. Du kan også sende filer ved å klikke på **Send** på **Verktøy**-menyen, velge filene og deretter klikke på **Send**.

Godta en fil fra en annen datamaskin.

Hvis en annen datamaskin i det administrative nettverket sender deg en fil, må du godta den ved å lagre den på datamaskinen din. Hvis EasyNetwork ikke kjører når en fil blir sendt til din datamaskin, vil du motta en melding i systemstatusfeltet helt til høyre for din oppgavelinje. Klikk på meldingen for å åpne EasyNetwork og få tilgang til filen.

- Klikk på **Mottatt**, og dra deretter filen fra EasyNetwork-innboksen til en mappe i Windows Utforsker.

Tips: Du kan også motta en fil fra en annen datamaskin ved å velge filen i EasyNetwork-innboksen og deretter klikke på **Godta** på **Verktøy**-menyen. I Godta-dialogboksen navigerer du til mappen der du vil lagre filen, velger den og klikker på **Lagre**.

Motta melding når en fil er sendt

Du kan motta en melding når en annen datamaskin i det administrative nettverket sender deg en fil. Hvis EasyNetwork ikke kjører, vil meldingen vises i systemstatusfeltet helt til høyre for din oppgavelinje.

1. Klikk på **Konfigurer** på **Alternativer**-menyen.
2. I Konfigurer-dialogboksen velger du boksen **Varsle meg når en annen datamaskin sender meg filer**.
3. Klikk **OK**.

KAPITTEL 45

Dele skrivere

Når du blir med i et administrativt nettverk, deler EasyNetwork lokale skrivere som er koblet til datamaskinen din, og bruker skriverens navn som det delte skrivernavnet. EasyNetwork oppdager også skrivere som deles av andre datamaskiner på nettverket, og tillater deg å konfigurere og bruke disse skriverne.

Hvis du har konfigurert en skriverdriver til å skrive ut gjennom en nettverksskriver (for eksempel en trådløs USB-skrivertjener), anser EasyNetwork skriveren som en lokal skriver, og deler den i nettverket. Du kan slutte å dele en skriver når som helst.

I dette kapitlet

Arbeide med delte skrivere 242

Arbeide med delte skrivere

EasyNetwork oppdager skrivere som deles av datamaskinene i nettverket. Hvis EasyNetwork oppdager en ekstern skriver som ikke er koblet til datamaskinen din, vises lenken **Tilgjengelige nettverksskrivere** i vinduet for delte filer når du åpner EasyNetwork for første gang. Dermed kan du installere tilgjengelige skrivere, eller avinstallere skrivere som allerede er koblet til datamaskinen din. Du kan også oppdatere listen over skrivere for å sikre at du viser oppdatert informasjon.

Hvis du ikke er logget på det administrative nettverket, men er koblet til det, kan du bruke skriverkontrollpanelet i Windows til å få tilgang til de delte skriverne.

Stanse deling av en skriver

Når du stanser deling av en printer, kan medlemmene ikke bruke den.

1. Klikk på **Skrivere** på **Verktøy**-menyen.
2. I dialogboksen for behandling av nettverksskrivere, velger du den skriveren du ikke lenger vil dele.
3. Klikk på **Ikke del**.

Installere en tilgjengelig nettverksskriver

Hvis du er medlem av et administrativt nettverk, har du tilgang til skrivere som deles. Du må imidlertid installere skriverdriveren som brukes av skriveren. Hvis eieren av skriveren slutter å dele sin printer, kan du ikke bruke den.

1. Klikk på **Skrivere** på **Verktøy**-menyen.
2. Velg et skrivernavn i dialogboksen for tilgjengelige nettverksskrivere.
3. Klikk på **Installer**.

Referanse

Ordlisten tar for seg og definerer de mest brukte sikkerhetstermene i McAfee-produkter.

Liste

8

802.11

Et sett med IEEE-standarder for å sende data over et trådløst nettverk. 802.11 er mest kjent som Wi-Fi.

802.11a

En utvidelse av 802.11 som sender data opp til 54 Mbit/s på 5 GHz-frekvens. Selv om overføringshastigheten er raskere enn 802.11b, er avstanden mye mindre.

802.11b

En utvidelse av 802.11 som sender data opp til 11 Mbit/s på 2,4 GHz-frekvens. Selv om overføringshastighten er lavere enn 802.11a, er avstanden større.

802.1x

En IEEE-standard for godkjenning på kablet og trådløst nettverk. 802.1x brukes vanligvis med 802.11 trådløse nettverk.

A

ActiveX-kontroller

En programvarekomponent som programmer eller websider bruker til å tilføye funksjonalitet som glir inn og fremstår som en normal del av programmet eller websiden. De fleste ActiveX-kontrollene er harmløse, men noen kan innhente informasjon fra datamaskinen.

administrert nettverk

Et hjemmenettverk med to typer medlemmer: administrerte medlemmer og ikke-administrerte medlemmer. Administrerte medlemmer tillater andre datamaskiner i nettverket å overvåke deres beskyttelsesstatus. Ikke-administrerte medlemmer gjør ikke det.

aktiveringspunkt

En geografisk grense dekket av et Wi-Fi (802.11) tilgangspunkt (AP). Brukere som kommer inn i et aktiveringspunkt med en trådløs datamaskin kan koble til Internett dersom aktiveringspunktet signaliserer (dvs. reklamerer for at det er der) og det ikke kreves godkjenning. Aktiveringspunkt finnes ofte på travle plasser som for eksempel flyplasser.

arkiv

For å opprette en kopi av viktige filer på CD, DVD, USB-stasjon, ekstern harddisk eller nettverksstasjon.

B

bibliotek

Elektronisk lagringsområde for filer som du har sikkerhetskopiert og publisert. Data Backup-biblioteket er et webområde på Internett og er tilgjengelig til alle med internettilgang.

bildefiltrering

Et alternativ for Foreldrestyring som blokkerer potensielt upassende webbilder fra å vises.

brannmur

Et system (maskinvare, programvare eller begge deler) som skal forhindre uautorisert tilgang til eller fra et privat nettverk. Brannmurer benyttes ofte til å forhindre at uautoriserte internettbrukere får tilgang til private nettverk som er koplet til Internett, spesielt et intranett. Alle beskjeder som går inn eller ut av intranettet passerer gjennom brannmuren, som undersøker hver beskjed og blokkerer de som ikke tilfredsstiller oppsatte sikkerhetskriterier.

buffer

Et midlertidig lagringsområde på datamaskinen. Nettleseren kan for eksempel hente en webside fra hurtiglageret (i stedet for en ekstern server) neste gang siden skal åpnes, og dermed sørge for raskere og mer virkningsfull navigering.

bufferoverløp

En tilstand som oppstår når mistenkelige programmer eller prosesser forsøker å lagre mer data i en buffer (midlertidig lagringsområde) på datamaskinen enn det er plass til. Bufferoverløp ødelegger eller overskriver data i nærliggende buffere.

båndbredde

Datamengden som kan overføres i en avgrenset tidsperiode.

D

DAT

(Datasignaturfiler) Filer som inneholder definisjonene som brukes til å oppdage virus, trojanske hester, spion- og reklameprogrammer og andre potensielt uønskede programmer på datamaskinen eller USB-stasjonen.

database for sikkerhetskopi på nettet

Plasseringen på nettjeneren der filene lagres etter en sikkerhetskopiering.

dele

Å gi e-postmottakere tilgang til utvalgte, sikkerhetskopierte filer i en begrenset tid. Når du deler en fil, sender du en sikkerhetskopi av filen til en spesifisert e-postmottaker. Mottakerne får en e-postmelding fra Data Backup som indikerer at filene er delt med dem. E-posten inneholder også en kobling til de delte filene.

delt hemmelighet

Streng eller nøkkel (vanligvis et passord) som deles mellom to kommuniserende parter før kommunikasjonen starter. En delt hemmelighet brukes til å beskytte sensitive deler av RADIUS-meldinger.

DNS

(Domenenavnsystem) Et system som konverterer vertsnavn eller domenenavn til IP-adresser. På Internett brukes DNS til å konvertere lettleste web-adresser (for eksempel www.myhostname.com) til IP-adresser (for eksempel 111.2.3.44), slik at webområdet kan gjenopprettes. Uten DNS ville du være nødt til å taste inn IP-adressen i webleseren.

DNS-tjener

(Domenenavnsystem-server) En datamaskin som sender tilbake IP-adressen tilknyttet et verts- eller domenenavn. Se også DNS.

domene

Et lokalt delnettverk eller en nøkkel for områder på Internett.

På et lokalt nettverk (LAN) er et domene et delnettverk som består av klient- og servermaskiner som kontrolleres av en sikkerhetsdatabase. I denne sammenhengen kan domener forbedre ytelsen. På Internett er et domene en del av en webadresse (for eksempel, i www.abc.com er abc domenet.

E

e-post

(elektronisk post) Beskjeder som sendes og mottas elektronisk over et datanettverk. Se også Webmail.

e-postklient

Et program du kjører på datamaskinen for å sende og motta e-post (for eksempel Microsoft Outlook).

ekstern harddisk

En harddisk som lagres utenfor datamaskinen.

ESS

(Extended Service Set) Et sett med to eller flere nettverk som danner et enkelt delnettverk

F

filfragmenter

Filrester som er spredt på en stasjon. Filfragmentering oppstår når filer legges til eller slettes, og kan gjøre at datamaskinens ytelse blir langsommere.

Foreldrestyring

Innstillinger som hjelper deg med å regulere hva barna dine kan se og gjøre på Internett. For å konfigurere Foreldrestyring kan du aktivere eller deaktivere bildefiltrering, velge en innholdsklassifisert gruppe og stille inn tidsbegrensninger på weblesning.

fullstendig arkivering

Hvis du vil arkivere et fullstendig datasett basert på filtypene og plasseringene du har konfigurert. Se også hurtigarkivering.

G

gjenopprette

Hente en kopi av en fil fra databasen for online-sikkerhetskopiering eller et arkiv.

godkjenning

En prosess som identifiserer en person – vanligvis via et brukernavn og passord.

H

hendelse

En handling satt i gang av enten brukeren, en enhet eller datamaskinen selv som utløser en reaksjon. McAfee registrerer hendelser i hendelsesloggen.

hjemmenettverk

To eller flere datamaskiner som er koblet sammen i et hjem slik at de kan dele filer og Internett-tilgang. Se også LAN.

hurtigarkivering

Arkivere kun de filene som har endret seg siden forrige fullstendige arkivering eller hurtigarkivering. Se også fullstendig arkivering.

hviteliste

En liste over webområder som brukere får tilgang til fordi webområdene ikke anses som farlige.

I

informasjonskapsel

En liten fil som inneholder informasjon, vanligvis med brukernavn og gjeldende dato og klokkeslett, som en person som navigerer på nettet har lagret på maskinen. Informasjonskapsler brukes i all hovedsak av webområder til å identifisere brukere som tidligere har registrert seg på eller besøkt området, men de kan også være en kilde til informasjon for hackere.

innholdsklassifiserte grupper

I Foreldrestyring er det en aldersgruppe som en bruker tilhører. Innholdet er tilgjengelig eller blokkert basert på hvilken innholdsklassifisert gruppe brukeren tilhører. Innholdsklassifiserte grupper omfatter: Småbarn, Barn, Unge ungdommer, Eldre ungdommer og Voksne.

integrert gateway

En enhet som kombinerer funksjonene til et tilgangspunkt, en ruter og en brannmur. Noen enheter har også ekstra sikkerhet og mellomegenskaper.

Internett

Internett består av et stort antall nettverk som er koblet sammen, og som bruker TCP/IP-protokoller til å finne og overføre data. Internett ble utviklet fra en sammenkopling av universitets- og høyskoledatamaskiner (på slutten av 1960-tallet og tidlig på 1970-tallet) finansiert av det amerikanske forsvarsdepartementet. Dette ble den gang kalt ARPANET. Dagens Internett er et verdensomspennende nettverk av nesten 100 000 uavhengige nettverk.

intranet

Et privat nettverk av datamaskiner, vanligvis innen en organisasjon, som kun godkjente brukere har tilgang til.

IP-adresse

Identifikasjonen til en datamaskin eller enhet på et TCP/IP-nettverk. Nettverk som bruker TCP/IP-protokoll, sender meldinger basert på IP-adressen til mottakeren. Formatet til en IP-adresse er en 32-biters numerisk adresse som skrives som fire numre atskilt med punktum. Hvert nummer kan være mellom 0 og 250 (for eksempel 192.168.1.100).

IP-forfalskning

Å forfalske IP-adressene i en IP-pakke. Dette brukes i mange typer angrep, blant annet kapring. Det brukes også ofte til å forfalske e-posthoder i spampost slik at de ikke kan spores.

isolere

Å isolere. I VirusScan blir for eksempel mistenkelige filer oppdaget og isolert slik at de ikke kan skade datamaskinen eller filer.

K

klarert liste

Inneholder elementer som du har klarert og som ikke oppdages. Hvis du klarerer et element (for eksempel et potensielt uønsket program eller en registerendring) ved et uhell, eller du vil at elementet skal kunne oppdages igjen, må du fjerne det fra listen.

klient

Et program som kjører på en PC eller arbeidsstasjon og er avhengig av en tjener for å utføre visse oppgaver. Et e-postprogram er for eksempel et program som gjør at du kan sende og motta e-post.

komprimering

En prosess der filer komprimeres til en form som minimerer plassen som kreves for lagring eller overføring.

kryptering

En prosess der data omformes fra tekst til kode, og informasjonen skjules slik at den ikke kan leses av folk som ikke vet hvordan de skal dekryptere den. Kryptert data kalles også krypteringstekst.

krypteringstekst

kryptert tekst. Krypteringstekst er uleselig før den konverteres til vanlig tekst (dekryptert).

L

LAN

(Lokalt nettverk) Et nettverk av datamaskiner som strekker seg over et relativt lite område (for eksempel en enkelt bygning). Datamaskiner på et LAN-nettverk kan kommunisere med hverandre og dele ressurser som skrivere og filer.

launchpad

En U3-grensesnittskomponent som fungerer som startpunkt for oppstart og administrasjon av U3 USB-programmer.

M

MAC-adresse

(Media Access Control address) Et unikt serienummer som er tildelt en fysisk enhet som har tilgang til nettverket.

man-in-the-middle-angrep

Metode for å fange opp og muligens endre beskjeder mellom to parter uten at noen av partene vet at kommunikasjonskoblingen har blitt brutt.

MAPI

(Messaging Application Programming Interface) Spesifikasjon for Microsoft-grensesnittet som gjør det mulig for ulike meldings- og arbeidsgruppeprogrammer (som e-post, talemelding og faks) å jobbe sammen via en enkelt klient, som Exchange.

message authentication code (MAC)

Sikkerhetskode som brukes til å kryptere meldinger som overføres mellom datamaskiner. Meldingen godkjennes hvis datamaskinen finner at den krypterte koden er gyldig.

midlertidig fil

En fil som er opprettet i minnet eller på en stasjon av operativsystemet eller et annet program. Den skal brukes i en økt, og deretter forkastes.

MSN

(Microsoft Network) Gruppe webbaserte tjenester som tilbys av Microsoft Corporation, bl.a. søkemotor, e-post, direktemeldinger og portal.

N

nettverk

En samling tilgangspunkter og brukerne som er tilknyttet dem. Tilsvarer ESS.

nettverkskart

Grafisk representasjon av datamaskinene og komponentene som utgjør et hjemmenettverk.

nettverksstasjon

En disk- eller båndstasjon som er koplet til en tjener på et nettverk som deles av flere brukere. Nettverkstasjoner kalles også eksterne stasjoner.

NIC

(Network Interface Card) Et kort som settes i en bærbar datamaskin eller en annen enhet, og kopler enheten til et lokalnett.

node

En enkelt datamaskin som er koblet til et nettverk.

nøkkel

En serie med bokstaver og siffer som brukes av to enheter til å autentisere kommunikasjonen. Begge enheter må ha nøkkelen. Se også WEP, WPA, WPA2, WPA-PSK, og WPA2- PSK.

nøkkelord

Et ord som du kan tilordne en sikkerhetskopiert fil, for å etablere et forhold eller en tilkopling til andre filer som har samme nøkkelord tilordnet. Tilordning av nøkkelord gjør det enklere å søke etter filer som du har publisert på Internett.

O

omfattende oppsiktsplassering

En mappe på din datamaskin som overvåkes for endringer ved sikkerhetskopiering Hvis du oppretter en omfattende oppsiktsplassering, tas oppsiktsfilene i den mappen og undermappene med i sikkerhetskopier.

oppringingsprogram

Programvare som hjelper deg med å opprette en Internett-tilkobling. Hvis det brukes med ondsinnede hensikter kan oppringingsprogrammer omdirigere Internett-tilkoblingene til andre enn din standard tjenesteleverandør av Internett (ISP) uten å informere deg om ytterlige kostnader.

oppsiktsfiler

Filtyper (for eksempel .doc, og .xls) som Data Backup sikkerhetskopierer eller arkiverer i oppsiktsplasseringer.

oppsiktsplasseringer

Mappene på datamaskinen din som Data Backup overvåker.

ordbokangrep

En type brute force-angrep som benytter vanlige ord for å forsøke å oppdage et passord.

orm

Reproduserende virus som finnes i aktivt minne, og som kan sende kopier av seg selv via e-postmeldinger. Ormer kan kopiere og legge beslag på systemressurser, noe som reduserer ytelsen eller stopper oppgaver.

overfladiske oppsiktsplasseringer

En mappe på din datamaskin som overvåkes for endringer av Data Backup. Hvis du oppretter en overfladisk oppsiktsplassering, tar Data Backup oppsiktsfilene i den mappen med i sikkerhetskopier, men undermappene tas ikke med.

P

Papirkurv

Simulert søppelbøtte for slettede filer og mapper i Windows.

passord

Kode (består vanligvis av bokstaver og tall) som brukes til å få tilgang til datamaskinen, et program eller et webområde.

passordhvelv

Et sikkert lagringsområde for dine passord. Her kan du lagre passordene dine og være sikker på at ingen andre brukere (selv en administrator) kan få tilgang.

phishing

Internettsvindel som er laget for å få tak i verdifull informasjon (som kredittkort- og personnummer, bruker-ID og passord) fra uvitende personer til bruk i bedrageri.

plugin-moduler

Et lite program som kobles til et større program for å gi ekstra funksjonalitet. For eksempel gir plugin-moduler webleseren tilgang til å starte filer innbygd i HTML-dokumenter som er i formater som webleseren vanligvis ikke kjenner igjen (for eksempel animasjons-, video- og lydfiler).

POP3

(Post Office Protocol 3) Grensesnitt mellom et e-postprogram om e-postserveren. De fleste hjemmebrukere har en POP3 e-postkonto, også kjent som standard e-postkonto.

popup-vinduer

Små vinduer som vises over andre vinduer på dataskjermen. Popup-vinduer brukes ofte til å vise reklame i weblesere.

port

Sted der informasjonen går inn og/eller ut av datamaskinen. For eksempel er et vanlig analogt modem tilkoblet en serieport.

potensielt uønsket program (PUP)

Program som samler inn og overfører personlig informasjon uten din tillatelse (for eksempel spion- og reklameprogrammer).

PPPoE

(Point-to-Point Protocol Over Ethernet) En måte å bruke Point-to-Point Protocol (PPP) oppringningsprotoll på med Ethernet som transport.

protokoll

Format (maskinvare eller programvare) for å overføre data mellom to enheter. Datamaskinene eller enheten må støtte den rette protokollen hvis du vil kommunisere med andre datamaskiner.

proxy

En datamaskin (eller programvaren som kjører på maskinen) som fungerer som en barriere mellom et nettverk og Internett ved å ha bare én enkelt nettverksadresse til eksterne områder. Ved å representere alle interne datamaskiner, beskytter proxyen nettverksidentiteter samtidig som den gir tilgang til Internett. Se også proxy-tjener.

proxy-tjener

En brannmurkomponent som styrer Internett-trafikk til og fra et lokalnett (LAN). En proxy-tjener kan forbedre ytelsen ved å levere data som brukerne ofte ber om, for eksempel en populær webside, og den kan filtrere og forkaste forespørsler som eieren ikke ønsker, for eksempel forespørsler om uautorisert tilgang til proprietære filer.

publisere

Gjøre en sikkerhetskopiert fil tilgjengelig for allmennheten på Internett. Du kan få tilgang til publiserte filer ved å søke i Data Backup-biblioteket.

R

RADIUS

(Remote Access Dial-In User Service) Protokoll som tillater godkjenning av brukere, som vanligvis har ekstern tilgang. Protokollen ble opprinnelig brukt for tjenere med ekstern tilgang via oppringning, men den brukes nå i en rekke godkjenningsmiljø, som 802.1x-godkjenning av WLAN-brukeres delte hemmelighet.

register

Database som Windows bruker til å lagre konfigurasjonsinformasjon. Registeret inneholder profiler for hver datamaskinbruker og informasjon om maskinvare, installerte programmer og egenskapsinnstillinger. Windows forsyner denne informasjonen med kontinuerlige henvisninger mens systemet kjører.

ren tekst

Tekst som ikke er kryptert. Se også kryptering.

roaming

Å gå fra et tilgangspunktområde til en annet uten forstyrrelser i tjeneste eller tilkoplingstap.

rootkit

En samling verktøy (programmer) som gir brukeren adgang til en datamaskin eller datamaskinnettverk på administrator-nivå. Rootkits kan omfatte spionprogrammer og andre potensielt uønskede programmer som kan medføre ytterligere risiko for datamaskinens sikkerhet og personlig informasjon.

ruter

En nettverksenhet som videresender datapakker fra et nettverk til et annet. Basert på interne rutertabeller leser rutere alle innkommende pakker og bestemmer hvordan de skal videresendes basert på kombinasjonen kilde og måladresse, samt gjeldende trafikkforhold (for eksempel last, linjekostnader og dårlige linjer). En ruter kalles av og til for et tilgangspunkt (AP).

råkraftsangrep (brute-force attack)

En metode for å tolke krypterte data, som f.eks. passord, gjennom inngående anstrengelse (rå kraft) i stedet for intellektuell strategi. «Brute force» anses som en ufeilbar, men tidkrevende, angrepsmetode. Brute force-angrep kalles også brute force-cracking.

S

sanntidssøk

Å gjennomsøke filer og mapper etter virus og annen aktivitet når de åpnes av deg eller datamaskinen.

sikkerhetskopi

For å opprette en kopi av viktige filer på en sikker, tilkoplet tjener.

skript

Liste over kommandoer som kan utføres automatisk (det vil si uten at bruker foretar seg noe). I motsetning til programmer lagres skript vanligvis som ren tekst og samles hver gang de kjøres. Makroer og batch-filer kalles også skript.

smartstasjon

Se USB-stasjon.

SMTP

(Simple Mail Transfer Protocol) En TCP/IP-protokoll for å sende meldinger fra en datamaskin til en annen på et nettverk. Denne protokollen brukes på Internett til å distribuere e-post.

snarvei

Fil som inneholder kun plasseringen til en annen fil på datamaskinen.

sporingsbilder

Små grafikkfiler som kan skjule seg på HTML-sider og tillater en uautorisert kilde å legge til informasjonskapsler på datamaskinen din. Disse informasjonskapslene kan da overføre informasjon til den uautoriserte kilden. Sporingsbilder kalles også skjulte/usynlige sporingsbilder.

SSID

(Service Set Identifier) Et tegn (hemmelig nøkkel) som identifiserer et Wi-Fi (802.11) nettverk. SSID konfigureres av nettverksadministrator og må oppgis av brukere som vil koble seg til nettverket.

SSL

(Secure Sockets Layer) En protokoll utviklet av Netscape for å sende private dokumenter via Internett. SSL bruker en offentlig nøkkel til å kryptere data som overføres over SSL-tilkoplingen. URL-er som krever en SSL-tilkobling begynner med https i stedet for http.

standard e-postkonto

Se POP3.

svarteliste

Innen anti-phishing en liste over webområder som ansees som farlige.

synkronisere

Løse uregelmessigheter mellom sikkerhetskopierte filer og dem som er lagret på den lokale datamaskinen. Du synkroniserer filer når filversjonen i databasen for sikkerhetskopi på nettet er nyere enn filversjonen på de andre datamaskinene.

systemgjenopprettingspunkt

En kopi av innholdet i datamaskinens minne eller en database. Windows lager gjenopprettingspunkt med jevne mellomrom og når det oppstår viktige systemhendelser (som når et program eller driver installeres). Du kan også opprette og sette navn på dine egne gjenopprettingspunkt når som helst.

SystemGuard

McAfee-varsler som oppdager uautoriserte endringer i datamaskinen og varsler deg når de oppstår.

søk på forespørsel

Søk som startes på forespørsel (dvs. når du setter i gang operasjonen). I motsetning til sanntidssøk startes ikke søk på forespørsel automatisk.

T

Tilgangspunkt

En nettverksenhet (vanligvis kalt en trådløs ruter) som kan kobles til en Ethernet-hub eller -svitsj for å utvide det fysiske serviceområdet til en trådløs bruker. Når trådløse brukere roamer med mobile enheter går overføringen fra ett Tilgangspunkt (AP) til et annet for å opprettholde tilkoblingen.

tjener

En datamaskin eller et program som tar imot tilkoblinger fra andre datamaskiner eller programmer og gir korrekte svar. For eksempel kobler e-postprogrammet seg til en e-posttjener hver gang du sender eller mottar meldinger.

tjenestenekt

En type angrep som stanser eller gjør trafikken i et nettverk langsommere. Et angrep av tjenestenekt (DoS-angrep) oppstår når et nettverk oversvømt av så mange tilleggsforespørsler at vanlig trafikk går langsommere eller avbrytes helt. Det resulterer vanligvis ikke i tyveri av informasjon eller andre sårbarheter i sikkerheten.

TKIP

(Temporal Key Integrity Protocol) Protokoll som adresserer svakhetene i WEP-sikkerheten, spesielt gjenbruken av krytperingsnøkler. TKIP endrer tidsbestemte nøkler for hver ti tusende pakke og sørger dermed for en dynamisk distribusjonsmetode som betydelig forbedrer nettverkssikkerheten. TKIP-sikkerhetsprosessen begynner med en 128-bits tidsbegrenset nøkkel som deles mellom klienter og tilgangspunkter. TKIP kombinerer den tidsbegrensede nøkkelen med klientmaskinens MAC-adresser og legger deretter til en relativ stor 16-oktetts initialiseringsvektor for å produsere nøkkelen som krypterer dataene. Denne prosessen sørger for at hver stasjon bruker forskjellig nøkkelflyt til å kryptere data. TKIP bruker RC4 til å utføre krypteringen.

trojansk hest

Program som fremstår som legitimt, men som kan skade verdifulle filer, forstyrre ytelsen og gi uautorisert tilgang til datamaskinen.

trådløst kort

Enhet som gir en datamaskin eller PDA trådløs kapasitet. Det kobles til via en USB-port, spor for PC-kort (CardBus) eller minnekort, eller internt til PCI-bussen.

trådløst PCI-kort

(Peripheral Component Interconnect) Trådløst kort som settes inn i PCI-sporet inni datamaskinen.

trådløst USB-kort

Trådløst kort som kan settes inn i USB-porten i datamaskinen.

U

U3

(Deg: Simplified, Smarter, Mobile) Plattform for å kjøre programmer for Windows 2000 eller Windows XP direkte fra en USB-stasjon. U3 ble startet i 2004 av M-Systems og SanDisk og lar brukere kjøre U3-programmer på en datamaskin med WIndows uten å installere eller lagre data eller innstillinger på datamaskinen.

uautorisert tilkoblingspunkt

Et uautorisert tilkoblingspunkt. Uautoriserte tilkoblingspunkt kan installeres på et sikkert firmanettverk for å gi uautoriserte parter tilgang til nettverket. De kan også lages for å la en angriper utføre et man-in-the-middle-angrep.

URL

(Uniform Resource Locator) Standardformatet for Internettadresser.

USB

(Universal Serial Bus) Et standardisert serielt datamaskingrensesnitt som du kan bruke til å koble eksterne enheter som tastatur, kontrollspaker og skrivere til datamaskinen.

USB-stasjon

En liten minnestasjon som kan kobles til USB-porten på en datamaskin. En USB-enhet fungerer som en liten harddisk, og gjør det enkelt å overføre filer fra en datamaskin til en annen.

V

virus

Reproduserende programmer som kan endre filer eller data. De gir ofte inntrykk av å komme fra en avsender du stoler på, eller ha et nyttig innhold.

VPN

(Virtual Private Network) Et privat nettverk konfigurert inni et offentlig nettverk for å utnytte administreringsmulighetene i det offentlige nettverket. VPN brukes av bedrifter for å opprette fjernnett (WANs) som rekker over store geografiske områder for å skaffe sted-til-sted-tilkoblinger til avdelingskontorer, eller for å la mobile brukere ringe opp bedriftens LAN-nettverk.

W

wardriver

Person som søket etter Wi-Fi (802.11)-nettverk ved å kjøre gjennom byer utstyrt med en Wi-Fi-datamaskin og en spesiell type maskinvare eller programvare.

webleser

Et program som brukes til å vise websider på Internett. Populære weblesere er bl.a. Microsoft Internet Explorer og Mozilla Firefox.

Webpost

Meldinger som sendes og mottas elektronisk over Internett. Se også e-post.

WEP

(Wired Equivalent Privacy) Krypterings- og godkjenningsprotokoll som defineres som en del av Wi-Fi (802.11)-standarden. De første versjonene er basert på RC4-chiffer og har betydelige svakheter. WEP prøver å ivareta sikkerheten ved å kryptere data over radiobølger slik at dataene er beskyttet mens de sendes fra et punkt til et annet. Man har imidlertid funnet ut at WEP ikke er like sikkert som man trodde.

Wi-Fi

(Wireless Fidelity) Et begrep som brukes av Wi-Fi Alliance når den referer til alle typer 802.11-nettverk.

Wi-Fi Alliance

En organisasjon bestående av ledende leverandører av trådløs maskin- og programvare. Wi-Fi Alliance bestreber seg på å sertifisere alle 802.11-baserte produkter for interoperabilitet og fremme begrepet Wi-Fi som det globale merkenavnet innenfor alle markeder for produkter for 802.11-baserte trådløse LAN-nettverk. Organisasjonen er et konsortium, testlaboratorium og finansinstitusjon for leverandører som vil fremme industrivekst.

Wi-Fi-godkjent

Å bli testet og godkjent av Wi-Fi Alliance. Wi-Fi-godkjente produkter anses som interoperable selv om de stammer fra forskjellige produsenter. En bruker med et Wi-Fi-godkjent produkt kan bruke et hvilket som helst tilkoplingspunkt-merke med et annet klientmaskinvare-merke som også er godkjent.

WLAN

(Wireless Local Area Network) Et lokalnettverk (LAN) som bruker en trådløs tilkobling. Et WLAN bruker høyfrekvensbølger i stedet for kabler til å la datamaskiner kommunisere med hverandre.

WPA

(Wi-Fi Protected Access) En spesifikasjonsstandard som gir økt databeskyttelse og tilgangskontroll for eksisterende og fremtidige trådløse LAN-systemer. WPA kjøres som en programvareoppgradering på eksisterende maskinvare, og er utledet fra og kompatibelt med IEEE 802.11i-standarden. Når WPA er installert på korrekt måte, kan brukere med trådløse lokalnettverk stole på at dataene deres er beskyttet, og at kun godkjente nettverksbrukere har tilgang til nettverket.

WPA-PSK

En spesiell WPA-modus utviklet for hjemmebrukere som ikke trenger like høy grad av sikkerhet som bedrifter, og som ikke har tilgang til godkjenningstjenere. I denne modusen oppgir hjemmebrukeren startpassordet manuelt for å aktivere WPA i modus for forhåndsdelt nøkkel, og bør endre passfrasen på hver trådløse datamaskin og hvert tilkoplingspunkt med jevne mellomrom. Se også WPA2-PSK og TKIP.

WPA2

En oppdatering til WPA-sikkerhetsstandarden, basert på 802.11i IEEE-standarden.

WPA2-PSK

En spesiell WPA-modus som ligner WPA-PSK og er basert på WPA2-standarden. En vanlig WPA2-PSK-funksjon er at enheten ofte støtter flere krypteringsmetoder (for eksempel AES, TKIP) samtidig, mens eldre enheter vanligvis kun støtter en krypteringsmetode av gangen (dvs. at alle klientene måtte bruke samme krypteringsmetode).

Om McAfee

McAfee, Inc., som har hovedkontor i Santa Clara i California og er verdensleder innen inntrengingsforhindring og håndtering av sikkerhetsrisikoer, leverer proaktive og dokumenterte løsninger og tjenester som ivaretar sikkerheten til systemer og nettverk over hele verden. Gjennom sin sikkerhetsekspertise og satsning på nyskaping gir McAfee hjemmebrukere, bedrifter, offentlig sektor og tjenesteleverandører mulighet til å stanse angrep, forhindre forstyrrelser og overvåke og forbedre sikkerheten kontinuerlig.

Copyright

Lisens

MELDING TIL ALLE BRUKERE: LES NØYE DEN AKTUELLE RETTSLIG BINDENDE AVTALEN SOM HØRER TIL LISENSEN DU KJØPTE, OG SOM ANGIR DE GENERELLE VILKÅRENE OG BETINGELSENE FOR BRUK AV DEN LISENSIERTE PROGRAMVAREN. HVIS DU IKKE VET HVILKEN LISENSTYPE DU HAR KJØPT, KAN DU SE I KJØPSBEVISET OG ANDRE RELATERTE LISENSTILDELINGER ELLER ORDREBEKREFTELSESDOKUMENTER SOM FØLGER MED PROGRAMVAREPAKKEN, ELLER SOM DU MOTTOK SEPARAT SOM EN DEL AV KJØPET (SOM EN BROSJYRE, EN FIL PÅ PRODUKT-CD-EN ELLER EN FIL PÅ WEBOMRÅDET DU LASTET NED PROGRAMVAREPAKKEN FRA). HVIS DU IKKE GODTAR ALLE VILKÅRENE SOM ANGIS I AVTALEN, MÅ DU IKKE INSTALLERE PROGRAMVAREN. DERSOM DET OVENNEVNTE ER TILFELLE, KAN DU RETURNERE PRODUKTET TIL MCAFEE, INC. ELLER TIL KJØPESTEDET OG FÅ KJØPESUMMEN REFUNDERT.

KAPITTEL 46

Kundestøtte og teknisk støtte

SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer så snart det oppdager dem. Kritiske beskyttelsesproblemer krever øyeblikkelig handling og kan sette din beskyttelsesstatus på spill (endre fargen til rød). Ikke-kritiske beskyttelsesproblemer krever ikke øyeblikkelig handling og kan kanskje sette din beskyttelsesstatus på spill (avhengig av hva slags type problem det dreier seg om). For å oppnå grønn beskyttelsesstatus må du reparere alle kritiske problemer og enten reparere eller ignorere alle ikke-kritiske problemer. Hvis du trenger hjelp til å diagnostisere beskyttelsesproblemene, kan du kjøre McAfee Virtuell Tekniker. For mer informasjon om McAfee Virtuell tekniker, se Hjelp for McAfee Virtuell tekniker.

Hvis du kjøpte sikkerhetsprogramvaren fra en annen samarbeidspartner eller forhandler enn McAfee åpner du en webleser og går til www.mcafeehjelp.com. Deretter velger du samarbeidspartner eller forhandler under Samarbeidskoblinger for å få tilgang til McAfee Virtuell tekniker.

Merknad: For å installere og kjøre McAfee Virtuell tekniker må du logge inn på datamaskinen din som Windows-administrator. Hvis du ikke gjør det, kan det hende MVT ikke kan løse problemene dine. For informasjon om hvordan du logger inn som Windows-administrator, se Hjelp for Windows. I Windows Vista™ blir du bedt om det når du kjører MVT. Når dette skjer klikker du på **Godta**. Virtuell tekniker virker ikke med Mozilla® Firefox.

I dette kapitlet

Bruke McAfee Virtuell tekniker 262
Støtte og nedlastninger.....263

Bruke McAfee Virtuell tekniker

I likhet med en personlig teknisk støtterepresentant, samler Virtuell tekniker informasjon om dine SecurityCenter-programmer, slik at den kan løse sikkerhetsproblemer på datamaskinen din. Når du kjører Virtuell tekniker sjekker det for å sikre at SecurityCenter-programmene dine virker som de skal. Hvis det oppdager problemer tilbyr Virtuell tekniker seg å fikse dem for deg eller gi deg mer detaljert informasjon om dem. Når den er ferdig, viser Virtuell tekniker resultatene av analysen og lar deg om nødvendig søke ytterligere teknisk støtte fra McAfee.

For å opprettholde sikkerheten og integriteten til datamaskinen og filene dine, samler ikke Virtuell tekniker inn personlig informasjon som kan identifisere deg.

Merknad: For mer informasjon om Virtuell tekniker, klikk **Hjelp** -ikonet i Virtuell tekniker.

Starte Virtuell tekniker

Virtual Technician samler informasjon om dine SecurityCenter-programmer slik at det kan hjelpe deg å løse dine beskyttelsesproblemer. so that it can help resolve your protection problems. For å sikre personvernet ditt inkluderer ikke denne informasjonen personlig, identifiserbar informasjon.

1. Under **Vanlige oppgaver** klikker du **McAfee Virtuell tekniker**.
2. Følg instruksjonene på skjermen for å laste ned og kjøre Virtuell tekniker.

Støtte og nedlastninger

Se følgende tabeller for webområder for McAfee Støtte og nedlastninger, inkludert brukerhåndbøker, for ditt land.

Støtte og nedlastninger

Land	McAfee støtte	McAfee nedlastninger
Australia	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
Brasil	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
Canada (engelsk)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Canada (fransk)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Kina (kinesisk)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
Kina (taiwansk)	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
Tsjekkoslovakia	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Danmark	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
Finland	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
Frankrike	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
Tyskland	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
Storbritannia	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
Italia	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
Japan	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
Korea	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
Mexico	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
Norge	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp
Polen	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp

Portugal	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
Spania	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
Sverige	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Tyrkia	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
USA	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

McAfee Totalbeskyttelse Brukerhåndbøker

Land	McAfee Brukerhåndbøker
Australia	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Canada (engelsk)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
Canada (fransk)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
Kina (kinesisk)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
Kina (taiwansk)	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
Tsjekkoslovakia	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Danmark	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
Frankrike	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
Tyskland	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
Storbritannia	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
Nederland	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf

Korea	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
Mexico	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Norge	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
Polen	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
Spania	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Sverige	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Tyrkia	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
USA	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

McAfee Internettsikkerhet Brukerhåndbøker

Land	McAfee Brukerhåndbøker
Australia	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
Canada (engelsk)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
Canada (fransk)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
Kina (kinesisk)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
Kina (taiwansk)	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Tsjekkoslovakia	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Danmark	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
Frankrike	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
Tyskland	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf

Storbritannia	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
Nederland	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
Mexico	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
Norge	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
Polen	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
Spania	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Sverige	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Tyrkia	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
USA	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

McAfee VirusScan Plus Brukerhåndbøker

Land	McAfee Brukerhåndbøker
Australia	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Canada (engelsk)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
Canada (fransk)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
Kina (kinesisk)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
Kina (taiwansk)	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
Tsjekkoslovakia	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf

Danmark	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
Frankrike	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
Tyskland	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Storbritannia	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
Nederland	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Mexico	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Norge	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
Polen	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
Spania	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Sverige	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
Tyrkia	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
USA	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

McAfee VirusScan Brukerhåndbøker

Land	McAfee Brukerhåndbøker
Australia	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
Canada (engelsk)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf

Canada (fransk)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
Kina (kinesisk)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
Kina (taiwansk)	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Tsjekkoslovakia	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Danmark	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
Frankrike	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
Tyskland	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Storbritannia	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
Nederland	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
Mexico	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
Norge	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
Polen	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
Spania	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Sverige	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Tyrkia	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
USA	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

Se følgende tabell for webområder om McAfee Threat Center og Virusinformasjon i ditt land.

Land	Sikkerhetshovedkontor	Virusinformasjon
Australia	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brasil	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
Canada (engelsk)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Canada (fransk)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Kina (kinesisk)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
Kina (taiwansk)	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Tsjekkoslovakia	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Danmark	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
Finland	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
Frankrike	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
Tyskland	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Storbritannia	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
Nederland	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
Italia	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
Japan	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
Korea	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
Mexico	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
Norge	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo
Polen	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo
Portugal	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo

Spania	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Sverige	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Tyrkia	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
USA	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

Se følgende tabell for HackerWatch-webområder i ditt land.

Land	HackerWatch
Australia	www.hackerwatch.org
Brasil	www.hackerwatch.org/?lang=pt-br
Canada (engelsk)	www.hackerwatch.org
Canada (fransk)	www.hackerwatch.org/?lang=fr-ca
Kina (kinesisk)	www.hackerwatch.org/?lang=zh-cn
Kina (taiwansk)	www.hackerwatch.org/?lang=zh-tw
Tsjekkoslovakia	www.hackerwatch.org/?lang=cs
Danmark	www.hackerwatch.org/?lang=da
Finland	www.hackerwatch.org/?lang=fi
Frankrike	www.hackerwatch.org/?lang=fr
Tyskland	www.hackerwatch.org/?lang=de
Storbritannia	www.hackerwatch.org
Nederland	www.hackerwatch.org/?lang=nl
Italia	www.hackerwatch.org/?lang=it
Japan	www.hackerwatch.org/?lang=jp
Korea	www.hackerwatch.org/?lang=ko
Mexico	www.hackerwatch.org/?lang=es-mx
Norge	www.hackerwatch.org/?lang=no
Polen	www.hackerwatch.org/?lang=pl
Portugal	www.hackerwatch.org/?lang=pt-pt
Spania	www.hackerwatch.org/?lang=es
Sverige	www.hackerwatch.org/?lang=sv
Tyrkia	www.hackerwatch.org/?lang=tr

USA	www.hackerwatch.org

Indeks

8

802.11 244
802.11a....244
802.11b 244
802.1x....244

A

ActiveX-kontroller 244
Administrere datamaskintilkoblinger ..103
Administrere din McAfee-konto....11
Administrere en enhet....223
Administrere nettverket eksternt 221
Administrere programmer og tillatelser 89
Administrere sikkerhetsnivåer i Firewall 78
administrert nettverk 244
Aktivere Smarte anbefalinger 82
Aktivere SystemGuards-beskyttelse....47
aktiveringspunkt....244
Analysere innkommende og utgående trafikk 119
Angi sikkerhetsnivået til Høy 80
Angi sikkerhetsnivået til Klarering 80
Angi sikkerhetsnivået til Sperr 79
Angi sikkerhetsnivået til Standard....80
Angi sikkerhetsnivået til Stealth 79
Angi sikkerhetsnivået til Åpen 81
Anti-Spam-funksjoner 125
Arbeide med arkiverte filer 187
Arbeide med delte skrivere 242
Arbeide med filtrert e-post....149
Arbeide med isolerte filer....62
Arbeide med isolerte programmer og informasjonskapsler 63
Arbeide med McAfee-brukere 157, 158
Arbeide med nettverkskartet 214
Arbeide med potensielt uønskede programmer 62
Arbeide med statistikk....114
Arbeide med søkeresultater 61
Arbeide med varsler....14, 23, 71
Arbeide med virus og trojanske hester...61
Arbeide med Windows-brukere 157
arkiv 244
Arkivere filer....179
Avbryte en automatisk arkivering 185

B

Behandle klarerte lister 53
Behandle systemtjenester....97
Bekreft abonnementet 11
Beskytt personlige opplysninger 172
Beskytte datamaskinen under oppstart. 84
Beskytte opplysninger på Internett....171
Beskytte passord....173
Beskytte personlige opplysninger 172
bibliotek 245
bildefiltrering....245
Blokkere et webområde 165
Blokkere Internett-tilgang for programmer 93
Blokkere tilgang for et program....93
Blokkere tilgang fra loggen for nylige hendelser 94
Blokkere tilgang til en eksisterende systemtjenesteport 99
Blokkere tilgangen for et nytt program..93
Blokkere webområder basert på nøkkelord....169
brannmur....245
Bruke alternativer for SystemGuards....46
Bruke klarerte lister 53
Bruke McAfee Virtuell tekniker 262
Bruke personlige filtre....141
Bruke SecurityCenter 7
Bruke utforskeren for lokal arkivering . 188
buffer....245
bufferoverløp 245
Bytt til Windows-brukere....158
båndbredde 245

C

Copyright 259

D

DAT....245
database for sikkerhetskopi på nettet..245
Deaktiver Anti-Spam-verktøylinjen....146
Deaktivere arkiveringskryptering og -komprimering 183
Deaktivere automatiske oppdateringer. 14
Deaktivere beskyttelse mot phishing...152
Deaktivere et spesialfilter 139

Deaktivere nøkkelordfiltrering 168
Deaktivere Smarte anbefalinger 82
Deaktivere spambeskyttelse 137
Definer tidsbegrensninger for bruk av Internett 164
Definere filtreringsalternativer 138
Definere innholdsklassifiseringsgruppe for en bruker 162
Definere innholdsklassifiseringsgruppen 161, 162
Definere tidsbegrensninger for bruk av Internett 164
Defragmentering av datamaskinen 198
dele 245
Dele filer 236
Dele og sende filer 235
Dele skrivere 241
delt hemmelighet 246
DNS 246
DNS-tjener 246
domene 246

E

EasyNetwork funksjoner 228
ekstern harddisk 246
Endre administratorpassordet for McAfee 160
Endre arkivplasseringen 183
Endre en systemtjenesteport 100
Endre et passord 174
Endre filtreringsnivået 138
Endre passord for passordhvelv 175
Endre tillatelsene til en administrert datamaskin 223
Endre visningsegenskapene til en enhet 223
Endring av diskdefragmenteringsoppgave 202
Endring av QuickClean-oppgave 200
e-post 246
E-postfiltrering 145
e-postklient 246
ESS 246

F

filfragmenter 246
Filtrer potensielt upassende webbilder 161
Filtrere potensielt upassende webbilder 161
Filtrere webområder 162, 165
Filtrere webområder med nøkkelord .. 165, 168
Fjern en McAfee-bruker 159
Fjerne en adressebok 133
Fjerne en klarert datamaskintilkobling 106
Fjerne en programtillatelse 95
Fjerne en systemtjenesteport 101
Fjerne en utestengt datamaskintilkobling 108
Fjerne en venn 136
Fjerne en webpostkonto 129
Fjerne et filtrert webområde 167
Fjerne et passord 175
Fjerne et personlig filter 142
Fjerne et webområde fra hvitelisten 152
Fjerne filer fra listen over manglende filer 191
Fjerne tilgangstillatelser for programmer 95
Foreldrestyring 246
Forlate et administrativt nettverk 234
Forstå beskyttelseskategorier 7, 9, 29
Forstå beskyttelsesstatus 7, 8, 9
Forstå beskyttelsestjenester 10
Forstå Network Manager-ikoner 211
Forstå webpostkontoinformasjon 128, 129
fullstendig arkivering 247
Funksjoner 178
Få nettverksinformasjonen til en datamaskin 116
Få programinformasjon 96
Få programinformasjon fra loggen for utgående hendelser 96
Få registreringsinformasjonen til en datamaskin 115
Få tilgang til nettverkskartet 214

G

Gi full tilgang fra loggen for nylige hendelser 91
Gi full tilgang fra loggen Utgående hendelser 91
Gi full tilgang til et program 90
Gi full tilgang til nytt et program 90
Gi nettverket nytt navn 215, 233
Gi tilgang til nettverket 231
Gjennomsøke datamaskinen 33, 57, 58
gjenopprette 247
Gjenopprette arkiverte filer 190
Gjenopprette en eldre filversjon fra et lokalt arkiv 191
Gjenopprette Firewall-innstillinger 88
Gjenopprette manglende filer fra et lokalt arkiv 190
godkjenning 247
Godta en fil fra en annen datamaskin .. 239

H

hendelse 247
Hendelseslogging 112
Hente frem administratorpassordet for McAfee 160
hjemmenettverk 247
hurtigarkivering 247
hviteliste 247
Håndtere arkiver 192
Håndtere informasjonsvarsler 75

I

Ignorere beskyttelsesproblemer 20
Ignorere et beskyttelsesproblem 20
informasjonskapsel 247
innholdsklassifiserte grupper 247
Installere en tilgjengelig nettverksskriver 242
Installere McAfee-sikkerhetsprogramvare på eksterne datamaskiner 225
integrert gateway 247
Internett 248
intranet 248
Invitere en datamaskin til å koble seg til det administrerte nettverket 217
IP-adresse 248
IP-forfalskning 248
isolere 248

K

Kjøre fullstendig arkivering og hurtigarkivering 184
Kjøre manuell arkivering 185
Klarere datamaskintilkoblinger 104
klarert liste 248
klient 248
Koble til det administrerte nettverket ..216
Koble til et administrert nettverk 217
komprimering 248
Konfigurere alternativer for manuelt søk 42
Konfigurere alternativer for sanntidssøk 40
Konfigurere alternativer for SystemGuards 47
Konfigurere automatiske oppdateringer 14
Konfigurere beskyttelse mot phishing .151
Konfigurere beskyttelsesstatusinnstillinger for Firewall 86
Konfigurere brukere 156
Konfigurere EasyNetwork 229
Konfigurere en ny systemtjenesteport ...99
Konfigurere Firewall-beskyttelse 77
Konfigurere innstillinger for hendelseslogg 112
Konfigurere innstillinger for pingforespørsler 85
Konfigurere inntrengingsoppdagelse 85
Konfigurere passordhvelvet 174
Konfigurere plassering for manuelt søk 44
Konfigurere Smarte anbefalinger for varsler 82
Konfigurere spamoppdagelse 137
Konfigurere systemtjenesteporter 98
Konfigurere søkealternativer i sanntid ..40
Konfigurere varslingsalternativer 26
Konfigurere venner 131
Konfigurere venner automatisk ... 132, 134
Konfigurere virusbeskyttelse 39, 57
Konfigurere webpostkontoer 127
Kopier eller slett en filtrert webpostmelding 150
Kopiere en delt fil 237
kryptering 248
krypteringstekst 248
Kundestøtte og teknisk støtte 261

L

LAN 249
launchpad 249
Legg til en McAfee-bruker 158
Legg til en venn manuelt 134
Legg til et domene 135
Legg til et personlig filter 141
Legge et webområdet til hvitelisten 151
Legge til en adressebok 132
Legge til en klarert datamaskin fra loggen for innkommende hendelser 105
Legge til en klarert datamaskintilkobling 104
Legge til en utestengt datamaskintilkobling 107
Legge til en venn fra Anti-Spam-verktøylinjen 134
Legge til en webpostkonto 127
Legge til et passord 174
Lisens 260
Logge på nettverket 231
Logge seg på et administrativt nettverk 230, 234
Logge, overvåke og analysere 111
Lære om Internett-sikkerhet 121
Lære om programmer 96
Løse beskyttelsesproblemer 8, 18
Løse beskyttelsesproblemer automatisk18

Løse beskyttelsesproblemer manuelt 19
Løse sikkerhetshull 224

M

MAC-adresse 249
Makulering av filer og mapper 207
Makulering av filer, mapper og disker .207
Makulering av hel disk 208
man-in-the-middle-angrep 249
MAPI 249
McAfee Anti-Spam 123
McAfee Data Backup 177
McAfee EasyNetwork 227
McAfee Internet Security 3
McAfee Network Manager 209
McAfee Personal Firewall 65
McAfee Privacy Service 153
McAfee QuickClean 193
McAfee SecurityCenter 5
McAfee Shredder 205
McAfee VirusScan 31
Merk en melding fra Anti-Spam verktøylinjen 145
message authentication code (MAC) ...249
midlertidig fil 249
Modifiser hvordan en melding blir behandlet og merket 141, 146
Motta melding når en fil er sendt 240
MSN 249

N

nettverk 249
nettverkskart 249
nettverksstasjon 249
Network Manager funksjoner 210
NIC 250
node 250
nøkkel 250
nøkkelord 250

O

Om diagrammet Trafikkanalyse 118
Om McAfee 259
Om SystemGuards-typer 48, 49
Om typer av klarerte lister 54
Om varsler 72
omfattende oppsiktsplassering 250
Oppdatere et filtrert webområde 166
Oppdatere nettverkskartet 214
Oppdatere SecurityCenter 13
Oppheve sperring av brannmuren øyeblikkelig 87
oppringingsprogram 250
oppsiktsfiler 250
oppsiktsplasseringer 250
Optimalisere Firewall-sikkerhet 84
ordbokangrep 250
orm 250
overfladiske oppsiktsplasseringer 250
Overvåke beskyttelsesstatusen til en datamaskin 222
Overvåke båndbredden for et program 119
Overvåke Internett-trafikk 118
Overvåke programaktivitet 119
Overvåke status og tillatelser 222

P

Papirkurv 251
passord 251
passordhvelv 251
Personal Firewall-funksjoner 66
phishing 251
Planlegge automatiske arkiveringer 184
Planlegge et søk 44
Planlegging av diskdefragmenteringsoppgave 201
Planlegging av oppgave 199
Planlegging av QuickClean-oppgave ...199
plugin-moduler 251
POP3 251
popup-vinduer 251
port 251
potensielt uønsket program (PUP) 251
PPPoE 251
Privacy Service-funksjoner 154
protokoll 251
proxy 252
proxy-tjener 252
publisere 252

Q

QuickClean-funksjoner 194

R

RADIUS 252
Rapportere spam til McAfee 149
Rediger en venn 135
Rediger et personlig filter 142
Rediger kontoinformasjon for en McAfee-bruker 159
Rediger områder i din hviteliste 152
Redigere en adressebok 132
Redigere en klarert datamaskintilkobling 105
Redigere en utestengt datamaskintilkobling 108
Redigere en webpostkonto 128
Redigere et domene 136

Referanse....243
register....252
ren tekst....252
Rens av datamaskinen....195, 197
Reparere eller ignorere beskyttelsesproblemer....8, 17
roaming....252
rootkit....252
ruter....252
råkraftsangrep (brute-force attack)....253

S

sanntidssøk....253
Se etter oppdateringer....13, 14
SecurityCenter-funksjoner....6
Sende en fil til en annen datamaskin....239
Sende filer til andre datamaskiner....239
Sette opp et administrert nettverk....213
Sette opp foreldrestyring....155
Shredder-funksjoner....206
sikkerhetskopi....253
Skjule informasjonsvarsler....75
Skjule velkomstskjermen ved oppstart....26
Skjule virusutbrudd-varsler....27
skript....253
Sletting av diskdefragmenteringsoppgave....203
Sletting av QuickClean-oppgave....201
Slutte å overvåke beskyttelsesstatusen til en datamaskin....222
Slutte å stole på datamaskiner i nettverket....219
smartstasjon....253
SMTP....253
snarvei....253
Sortere arkiverte filer....188
Sperre Firewall øyeblikkelig....87
Sperre og gjenopprette Firewall....87
Spesifisering av personlig filter....141, 142
Spille av en lyd med varsler....26
Spore en datamaskin fra loggen for innkommende hendelser....116
Spore en datamaskin fra loggen for inntrengingsoppdagelseshendelser....116
Spore en nettverksdatamaskin geografisk....115
Spore en overvåket IP-adresse....117
Spore Internett-trafikk....115
sporingsbilder....253
SSID....253
SSL....253
standard e-postkonto....253
Stanse deling av en skriver....242
Stanse deling av fil....236
Starte beskyttelse av direktemeldinger....37
Starte brannmurbeskyttelse....69
Starte e-postbeskyttelse....36
Starte Firewall....69
Starte HackerWatch-brukeropplæringen....122
Starte sanntids virusbeskyttelse....33
Starte skriptsøkbeskyttelse....36
Starte spionprogrambeskyttelse....36
Starte tilleggsbeskyttelse....35
Starte Virtuell tekniker....262
Stenge ute datamaskintilkoblinger....107
Stenge ute en datamaskin fra loggen for innkommende hendelser....109
Stenge ute en datamaskin fra loggen for inntrengingsoppdagelseshendelser....110
Stille inn arkiveringsalternativer....180
Stille inn filtyper for arkivering....182
Stoppe brannmurbeskyttelse....70
Stoppe sanntids virusbeskyttelse....33
Støtte og nedlastninger....263
svarteliste....254
synkronisere....254
systemgjenopprettingspunkt....254
SystemGuard....254
søk på forespørsel....254
Søke etter en arkivert fil....188
Søke etter en delt fil....237
Søkekriterier....237

T

Ta i bruk filtre for tegnsett....140
Ta med en plassering i arkivet....181
Tilbakestille passord for passordhvelv....176
Tilgangspunkt....254
Tillat bare utgående tilgang for et program....92
Tillat bare utgående tilgang fra loggen for utgående hendelser....92
Tillat bare utgående tilgang fra loggen Nylige hendelser....92
Tillat bare utgående tilgang til programmer....92
Tillat et webområde....166
Tillat Internett-tilgang for programmer....90
Tillat tilgang til en eksisterende systemtjenesteport....99
tjener....254
tjenestenekt....254
TKIP....255
trojansk hest....255
trådløst kort....255
trådløst PCI-kort....255
trådløst USB-kort....255

Åpne en arkivert fil 189

U

U3 255
uautorisert tilkoblingspunkt 255
URL 255
USB 255
USB-stasjon 255
Utelate en plassering fra arkivet 182

V

virus 256
VirusScan-funksjoner 32
Vis detaljer for et element 215
Vis eller skjul ignorerte problemer 20
Vis en hendelse for filtrert webpost 150
Vise alle hendelser 30
Vise bare Smarte anbefalinger 83
Vise eller skjule et element på nettverkskartet 215
Vise eller skjule informasjonsvarsler 24
Vise eller skjule informasjonsvarsler når du spiller 25
Vise et sammendrag av arkiveringssaktiviteten 192
Vise global Internett-portaktivitet 114
Vise hendelser 18, 29
Vise innkommende hendelser 113
Vise inntrengingsoppdagelseshendelser 113
Vise nylige hendelser 29, 112
Vise og skjule informasjonsvarsler 24
Vise statistikk for globale sikkerhetshendelser 114
Vise søkeresultater 58
Vise utgående hendelser 91, 113
Vise varsler når du spiller 75
VPN 256

W

wardriver 256
webleser 256
Webpost 256
WEP 256
Wi-Fi 256
Wi-Fi Alliance 256
Wi-Fi-godkjent 256
WLAN 257
WPA 257
WPA2 257
WPA2-PSK 257
WPA-PSK 257

Å

Åpne EasyNetwork 229